

# SSQ STRATEGIC STUDIES QUARTERLY

---

SPRING 2020

VOL. 14, NO. 1

---

## **Time for a Counter-AI Strategy**

M. A. Thomas

---

## **Success of Persistent Engagement in Cyberspace**

Jason Healey  
Stuart Caudill

---

## **FEATURE ARTICLE**

## **Artificial Intelligence: A Threat to Strategic Stability**

James S. Johnson

---

## **Three-Way Power Dynamics in the Arctic**

Rebecca Pincus

---

## **Strategic Choice and the Orbital Security Dilemma**

LTC Brad Townsend, USA

---

## **Strategic Contours of China's Arms Transfers**

Michael Raska  
Richard A. Bitzinger

---

## **Strategy in the New Era of Tactical Nuclear Weapons**

COL Joseph D. Becker, USA

---

---

# SSQ STRATEGIC STUDIES QUARTERLY

---

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

**Commander, Air Education and Training Command**  
Lt Gen Marshall B. Webb, USAF

**Commander and President, Air University**  
Lt Gen James B. Hecker, USAF

**Director, Academic Services**  
Mehmed Ali, PhD

**Director, Air University Press**  
Lt Col Darin Gregg, USAF

---

**Editor**  
Col W. Michael Guillot, USAF, Retired

**Managing Editor**  
Jeanne K. Shamburger

**Print Specialist**  
Megan N. Hoehn

**Illustrator**  
Daniel M. Armstrong

**Webmaster**  
Kevin V. Frey

---

## *Advisors*

Gen Michael P. C. Carns, USAF, Retired  
James W. Forsyth, 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*

David C. Benson, PhD  
Mark J. Conversino, PhD  
Kelly A. Grieco, PhD  
Michael R. Kraig, PhD  
Col Kristi Lowenthal, USAF, PhD  
Dawn C. Murphy, PhD  
David D. Palkki, PhD  
Nicholas M. Sambaluk, PhD



<https://www.af.mil/>



<https://www.aetc.af.mil/>



<https://www.airuniversity.af.edu/>

# STRATEGIC STUDIES QUARTERLY

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

---

SPRING 2020

VOL. 14, NO. 1

---

## POLICY FORUM

### 3 **Time for a Counter-AI Strategy**

M. A. Thomas

### 9 **Success of Persistent Engagement in Cyberspace**

Jason Healey

Stuart Caudill

## FEATURE ARTICLE

### 16 **Artificial Intelligence: A Threat to Strategic Stability**

James S. Johnson

## PERSPECTIVES

### 40 **Three-Way Power Dynamics in the Arctic**

Rebecca Pincus

### 64 **Strategic Choice and the Orbital Security Dilemma**

LTC Brad Townsend, USA

### 91 **Strategic Contours of China's Arms Transfers**

Michael Raska

Richard A. Bitzinger

### 117 **Strategy in the New Era of Tactical Nuclear Weapons**

COL Joseph D. Becker, USA

## BOOK REVIEWS

- 141 *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*  
by John P. Carlin with Garrett M. Graff  
Reviewed by Dr. Mark T. Peters II, USAF, Retired
- 142 *Nanoweapons: A Growing Threat to Humanity*  
by Louis A. Del Monte  
Reviewed by Maj Patrick M. Milott, USAF
- 144 *Unrivaled: Why America Will Remain the World's Sole Superpower*  
by Michael Beckley  
Reviewed by Brig Gen Chad Manske, USAF
- 146 *Cyber Security: Threats and Responses for Government and Business*  
by Jack Caravelli and Nigel Jones  
Reviewed by Dr. Mark T. Peters II, USAF, Retired
- 148 *Army of None: Autonomous Weapons and the Future of War*  
by Paul Scharre  
Reviewed by 1st Lt Nathaniel Lewis, USAF
- 149 *On the Brink: Trump, Kim, and the Threat of Nuclear War*  
by Van Jackson  
Reviewed by CMSgt Frank Murphy, USAF, Retired

## Time for a Counter-AI Strategy

The United States and China have each vowed to become the global leader in artificial intelligence (AI). In 2016, the United States published its National Artificial Intelligence Research and Development Strategic Plan. In 2017, China released its “New Generation Artificial Intelligence Development Plan,” announcing its intention to leapfrog the United States to become the global leader in AI by 2030 by combining government and private sector efforts.<sup>1</sup> The United States countered with the publication of the 2018 Department of Defense Artificial Intelligence Strategy, focused on maintaining AI leadership through faster innovation and adoption, and in 2019 updated its original plan.<sup>2</sup>

The competition has been characterized as an “AI arms race,” measured by expenditure, number of patents filed, or speed of adoption. On the battlefield, the perceived benefits of AI are increased speed and precision as AI systems rapidly handle tasks such as target identification, freeing humans for higher-level cognitive tasks. AI will, in theory, help the military to act faster, eclipsing its adversary’s ability to observe, orient, decide, and act.

The singular strategic focus on gaining and maintaining leadership and the metaphor of an “arms race” are unhelpful, however. Races are unidimensional, and the winner takes all. Previous arms races in long-range naval artillery or nuclear weapons were predicated on the idea that advanced tech would create standoff, nullifying the effects of the adversary’s weapons and deterring attack. But AI is not unidimensional; it is a diverse collection of applications, from AI-supported logistics and personnel systems to AI-enabled drones and autonomous vehicles. Nor does broadly better tech necessarily create standoff, as the US military learned from improvised explosive devices in Afghanistan. This means that in addition to improving its own capabilities, the United States must be able to respond effectively to the capabilities of others. In addition to its artificial intelligence strategy, the United States needs a counter-AI strategy.

### The AI Challenge

US competitors are already making military use of AI. In the military parade that marked the 70th anniversary of the Chinese Communist Party, the People’s Liberation Army displayed autonomous vehicles and drones.<sup>3</sup> At the same time, Russia is forging ahead with the Status-6, a nuclear autonomous torpedo.<sup>4</sup> Less capable countries will acquire AI-enabled weapons and systems through purchases or security cooperation.

The popular focus on military AI has been on tactical applications such as weapons targeting, and AI will be most successful when applied to static, simple problems. However, AI-enabled competitors and adversaries will develop new decision-making processes, modes of operation and coordination, battlefield capabilities, and weapons. Enterprise systems in human resources, logistics, procurement, equipment management and maintenance, accounting, intelligence collection and analysis, and reporting may also be AI-enabled. Operational and strategic leaders may turn to AI systems to suggest or test courses of action.

AI will likely create vulnerabilities as well as advantages. It may be error prone or biased, unpredictable, unreliable, opaque, and less capable of fine discrimination. Paul Scharre of the Center for a New American Security warns of the possibility of “a million mistakes a second” and rapid AI-enabled escalation of the kind illustrated by the 2010 Wall Street “flash crash” driven by automated trading programs.<sup>5</sup> Although he calls for a greater investment in testing to ensure the reliability of AI systems, AI may be intrinsically unreliable. For example, the problems to which AI is applied may be dynamic, or the AI itself may be constantly updated with new data.<sup>6</sup> Further, the interaction of multiple, different AI systems may produce unanticipated emergent behaviors.

Humans may hesitate to trust their own AIs—there is active research in developing “explainable AI” to foster human trust—but it is more likely that they will trust them too much.<sup>7</sup> Just as there is a generation of “digital natives” who grew up with computers, there will be a new generation of “AI natives” who are sophisticated users but take the technology for granted, do not know how it operates, do not understand its limitations, and lack the skills to operate without it. To the extent that they habitually use AI to tee up choices, it may be more difficult for them to generate creative options.

### **Strategic Counter-AI Initiatives**

A counter-AI strategy would seek to harden the United States as a target for AI-enabled attacks, reduce the advantages of AI to an adversary, and predict and adapt to changes in behavior that are consequences of reliance on AI. Among other measures, the United States could take more aggressive steps to protect US data that could be used for training AI models, invest in counter-AI tactics, and change how it comprehends AI behavior. Finally, the United States should cultivate self-awareness of the vulnerabilities created by its own increasing reliance on AI systems.

### ***Protect Relevant Data Sets***

The United States should seek to better protect sensitive data sets from adversaries that may use them to develop (“train”) AI models. A particularly damaging hack in the DOD occurred with the 2015 infiltration of the Office of Personnel Management in which an estimated 21.5 million personnel files were compromised, including the forms submitted by individuals to apply for or maintain the clearances that give them access to classified information.<sup>8</sup> Such data might be used to develop a predictive model for intelligence targeting that estimates the likelihood that a person has a high-level clearance.

At present, US policy on data protection is inconsistent. The executive order *Maintaining American Leadership in Artificial Intelligence* requires agencies to set as a strategic objective the enhancement of “access to high-quality . . . [f]ederal data [consistent with] safety, security, privacy and confidentiality protections.”<sup>9</sup> However, these criteria may not be sufficient because the information can be used to train models even if it is fully anonymized and so does not present privacy concerns.

The handling of private data is also a concern. A number of countries have passed data localization laws that require data collected in country to be stored in country.<sup>10</sup> Localization allows governments to set and enforce standards for the securitization and handling of private data that might otherwise be stored in extraterritorial servers. However, such laws also come at a price of reduced efficiency for global economic exchanges. Authoritarian governments may also use such laws to access their citizens’ data and enforce censorship.<sup>11</sup> India is debating data localization while the European Union has explicitly rejected it.<sup>12</sup>

The United States has also rejected localization. The United States Trade Representative has called out China, India, Indonesia, Kenya, Korea, Nigeria, Russia, Saudi Arabia, Turkey, and Vietnam for data restrictions that inhibit digital trade and impair global competitiveness.<sup>13</sup> But at the same time, the Committee on Foreign Investment in the United States has used authority under new legislation to prevent foreign acquisition of private data by, for example, forcing Chinese divestment from Grindr, a dating app that collects personal information.<sup>14</sup> Eric Rosenbach and Katherine Mansted of the Harvard Kennedy School Belfer Center for Science and International Affairs anticipate stepped-up cyberattacks by adversaries on data sets that can be used for training AI and call for a national information policy to protect data.<sup>15</sup>

### ***Invest in Counter-AI Tactics***

The United States should invest in research for counter-AI tactics. For example, research on adversarial images focuses on how to defeat AI image recognition systems, which can be thrown off course by subtle changes in the image to be analyzed. Researchers developed an image of a turtle classified by an AI program as a rifle and an image of a baseball classified as espresso.<sup>16</sup> Others have developed an AI program that can subtly tweak facial images to reduce the possibility of detection by AI facial recognition programs.<sup>17</sup> Slight physical defacements can defeat the ability of AI programs to recognize street signs. However, these approaches can be very specific to the implementation of the AI program that they seek to defeat.

More broadly, the United States must invest in developing methods to hack, crack, and outpace an adversary's AI by taking advantage of AI error and biases, the inability of AI to adapt to novelty, and the vulnerability of channels used for developing and pushing software updates. Exploiting such flaws would involve identifying where adversaries rely on AI and for what purposes, reverse engineering AI systems, red teaming the likely decisions of AI programmers (by, for example, identifying the likely source of training data or the algorithms used), and using generative adversarial nets—programs that seek the limits of AI classification abilities. Expertise in counter-AI tactics should be co-located with expertise in offensive cyber capabilities. Tactical counter-AI may need offensive cyber to open the door to AI-enabled systems or to block or spoof pushed software updates, while cyber may need AI expertise to take on AI-enabled cyber adversaries.

### ***Change How We Predict and Understand Adversary Behavior***

Analysts charged with assessing and anticipating competitor and adversary behavior will need new approaches. As illustrated by the work on adversarial images, AI programs make mistakes no human would make—which will make those who rely on them less predictable. Sherman Kent, the famed CIA intelligence analysis pioneer, explained why the Central Intelligence Agency estimates during the Cuban missile crisis gave no credence to the idea that Khrushchev had put missiles in Cuba. He wrote, “It is when the other man zigs violently out of the track of ‘normal’ behavior that you are likely to lose him. If you lack hard evidence of the prospective erratic tack and the zig is so far out of line as to seem to you to be suicidal, you will probably misestimate him every time.”<sup>18</sup> It will also become more difficult to ascribe intentionality to adversary actions, a particular concern in situations that may be escalatory. At the same time, the



United States should consider that competitors and adversaries seeking to understand US behavior will have identical challenges.

The current strategy of the United States assumes that AI leadership will ensure dominance and deter. The reality of AI is more complicated and ambiguous. The United States needs to consider how it will deal effectively with competitors and adversaries that rely on AI and how it will address the vulnerabilities that arise from its own increasing reliance. **SSQ**

**M. A. Thomas**

Professor, US Army School of Advanced  
Military Studies

### Notes

1. Elsa Kania, "China's AI Agenda Advances," *The Diplomat*, 14 February 2018, <https://thediplomat.com/>.
2. US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: US Department of Defense, 2019), <https://media.defense.gov/>.
3. Patrick Tucker, "New Drones, Weapons Get Spotlight in China's Military Parade," *Defense One*, 1 October 2019, <https://www.defenseone.com/>.
4. Franz-Stefan Gady, "Russia's New Nuclear Torpedo-Carrying Sub to Begin Sea Trials in June 2020," *The Diplomat*, 10 September 2019, <https://thediplomat.com/>.
5. Paul Scharre, "A Million Mistakes a Second," *Foreign Policy*, 12 September 2018, <https://foreignpolicy.com/>.
6. Paul Scharre, "Killer Apps: The Real Dangers of an AI Arms Race," *Foreign Affairs*, May/June 2019, <https://www.foreignaffairs.com/>.
7. See, for example, Matt Turek, "Explainable Artificial Intelligence (XAI)," Defense Advanced Research Projects Agency, accessed 9 October 2019, <https://www.darpa.mil/>.
8. Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," *Wired*, 23 October 2016, <https://www.wired.com/>.
9. Executive Order 13859 of 11 February 2019, Maintaining American Leadership in Artificial Intelligence, 84 Fed. Reg. 3967–3972 (19 February 2019), <https://www.federalregister.gov/>.
10. Samm Sacks, "New China Data Privacy Standard Looks More Far-Reaching Than GDPR," Center for Strategic and International Studies, 29 January 2018, <https://www.csis.org/>; Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cyber-security Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina* (blog), *New America*, 29 June 2018, <https://www.newamerica.org/>; and Benny Bogaerts and Kara Segers, "The 'Localisation' of Russian Citizens' Personal Data," KPMG, 5 September 2018, <https://home.kpmg/>.
11. See, for example, Matthew Newton and Julia Summers, "Russian Data Localization Laws: Enriching 'Security' & the Economy," The Henry M. Jackson School of International Studies, University of Washington, 28 February 2018, <https://jsis.washington.edu/>.

12. Ronak D. Desai, "India's Data Localization Remains a Key Challenge for Foreign Companies," *Forbes*, 6 October 2019, <https://www.forbes.com/>; "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)," Pub. L. No. 32016R0679, 119 OJ L (2016), *Official Journal of the European Union*, <http://data.europa.eu/>; and "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Text with EEA Relevance)," Pub. L. No. 32018R1807, 303 OJ L (2018), *Official Journal of the European Union*, <http://data.europa.eu/>.
13. Office of the United States Trade Representative, "Fact Sheet on 2019 National Trade Estimate: Key Barriers to Digital Trade," March 2019, <https://ustr.gov/>.
14. Nevena Simidjijaska, "CFIUS Flexes New Muscles Where Customer Data and Critical Technology Are Involved," *Corporate Compliance Insights*, 24 April 2019, <https://www.corporatecomplianceinsights.com/>.
15. Eric Rosenbach and Katherine Mansted, "How to Win the Battle over Data," *Foreign Affairs*, 17 September 2019, <https://www.foreignaffairs.com/>.
16. Anish Athalye et al., "Synthesizing Robust Adversarial Examples," *arXiv:1707.07397v3 [Cs.CV]*, 7 June 2018, <http://arxiv.org/>.
17. A. J. Bose and P. Aarabi, "Adversarial Attacks on Face Detectors Using Neural Net Based Constrained Optimization," in Institute of Electrical and Electronics Engineers (IEEE), *2018 IEEE 20th International Workshop on Multimedia Signal Processing (MMSP)*, Vancouver, BC, 29–31 August 2018 (Piscataway, NJ: IEEE, 2018), 1–6, <https://doi.org/10.1109/MMSP.2018.8547128>.
18. Sherman Kent, "A Crucial Estimate Relived," *Studies in Intelligence* 8, no. 2 (Spring 1964): 1–18, posted to CIA Library website 19 March 2007, <https://www.cia.gov/>.

## Success of Persistent Engagement in Cyberspace

The US Department of Defense's 2018 cyber strategy is the most important development in this arena in the past 20 years.<sup>1</sup> It recognizes that states are continuously engaged in cyber operations and prescribes an imperative to "persistently contest" adversaries "in day-to-day competition" by, among other things, "defending forward to intercept and halt cyber threats."<sup>2</sup> Persistent engagement is straightforward yet subtle. Countering malicious cyber activity below the level of armed conflict requires daily interaction and competition to "expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins."<sup>3</sup> US Cyber Command (USCYBERCOM) must consistently conduct operations to impose just enough friction on adversaries to moderate their behavior but not such disruption as to induce further attacks.

Academics and policy makers have debated the merits of persistent engagement, and perhaps it is indeed the correct strategy to deal with cyber conflict. However, as with the introduction of any new strategy, developing it is trivial compared to implementing it effectively against a competent adversary. At a minimum, persistent engagement requires (1) strong and sustained military and civilian leadership that embraces the strategy; (2) an organized, trained, and equipped force; (3) clear signaling to adversaries; (4) the trust of international and domestic partners; and (5) a robust interagency process. While the DOD might have the leadership and forces required to succeed, it is far from clear that the interagency process, the trust of partners, and signaling are or will be in place soon given the current political climate. Thus, the gains from persistent engagement will likely not be as significant as expected and will have a greater risk of encouraging, not discouraging, adversary attacks.

### Strong and Sustained Leadership

Military strategies are useless without strong military and civilian leadership to implement and direct them—not just today but over the years (or even decades) needed for success. There is widespread agreement that USCYBERCOM commander Gen Paul Nakasone is an exceptionally well-qualified military leader.<sup>4</sup> His staff and subordinates are equally well regarded.

Nonetheless, there are reasons for concern. First, it is not clear that leadership above the operational command understands the strategy and subtlety persistent engagement requires. In his confirmation testimony for appointment as chairman of the Joint Chiefs, Gen Mark Milley asserts that in cyberspace “a good offense is critical, and that is the best defense”—which may be true but is not the same as persistent engagement.<sup>5</sup> This framing is similar to that of the White House and some members of Congress.

Second, the next cyber commanders may not embrace persistent engagement as fully as has General Nakasone. Continuity is more likely if the next generation gives rise to Nakasone protégés, but the next commander may be a more traditional war-fighting general eager to take the fight aggressively to the enemy. The instinct of many warriors is to triple down on aggression, losing not just the subtlety at the heart of the strategy but the strategy itself.

### **Effectively Organized, Trained, and Equipped Force**

The United States is well along in having a properly organized, trained, and equipped cyber force. USCYBERCOM’s Cyber Mission Force (CMF) is at full operational capability with 133 teams comprising over 6,000 personnel.<sup>6</sup> These teams have been operationally engaged against the Islamic State and Russian interference during the 2018 midterm elections.<sup>7</sup> While they demonstrate significant capability, the CMF is not without its issues. Just five months after reaching full operational capability, many teams no longer met training standards.<sup>8</sup> Given the high tempo of operations suggested by the new strategy, USCYBERCOM will be hard-pressed to keep enough trained personnel, infrastructure, and capabilities over the years or decades.

### **Clear Signaling to Adversaries**

Perhaps the most important prediction of persistent engagement is that adversaries will learn which of their operations are far enough outside the norm as to invite significant US response. Michael Fischerkeller, a researcher at the Institute of Defense Analyses, and Richard Harknett, Political Science Department head at the University of Cincinnati, write about tacit bargaining such that over time each side will come to understand the “boundaries or limits on behaviors.”<sup>9</sup> Operations that support persistent engagement are essentially a never-ending series of signals to shepherd adversaries toward preferred US norms.

Communicating intent in cyberspace is inherently difficult because operations are usually hidden and denied while offensive attacks, pre-attack reconnaissance, and espionage are hard to distinguish.<sup>10</sup> Former National Security Agency (NSA) deputy director Chris Inglis notes that misreading “a limited action [such as routine espionage] as an existential threat” could lead to “escalating a situation in a manner unintended by the attacker.”<sup>11</sup> Despite this risk, there is a near total lack of communication between adversaries outside the arena of competition itself, inviting mistake and miscalculation. There is no direct contact between the DOD and the Chinese military as China’s leadership is still incensed over a signaling attempt: the US indictment of five Chinese cyber officers. There is also no direct contact between US and Russian militaries, though at least there are hotlines to connect the White House with the Kremlin and between each side’s computer emergency response teams.<sup>12</sup>

Hawkish rhetoric creates further uncertainty about US intentions. While US Cyber Command discusses persistent engagement primarily as a defensive strategy, the White House thinks of it as an offensive one. This gap will magnify the opportunities for mistake and miscalculation.

Even if adversaries detect and understand US signals, they may not be sure that the punishment will stop if they comply with US preferences.<sup>13</sup> Could Russia’s or China’s leadership be confident that if it moderated its cyber operations against the United States, its respective countries might not still suffer covert action, espionage, indictments, sanctions, or “hostile” cross-border information that threaten regime stability?

### **Trust of International and Domestic Partners**

The new strategy recognizes the importance of partnerships, emphasizing that the DOD “will collaborate with our interagency, industry, and international partners to advance our mutual interests.”<sup>14</sup> However, there are conflicting interests as well as mutual interests in stopping adversary cyber operations. Persistent engagement and forward defense blur the lines between adversary (red space), US (blue space), and other networks (gray space). With these euphemisms, it can be easy to forget that gray space is typically shorthand for someone else’s property physically located in a country with which the United States is at peace.

Previously, cyber operations that would deliver an effect in red or gray space required extensive interagency coordination, often the approval of the president.<sup>15</sup> Under this new strategy, and related authorizations by Congress and the White House, US cyber forces will have more freedom

of action to pivot with adversaries and disrupt threats in or through the networks of friendly nations.<sup>16</sup>

As Max Smeets of the Center for Security Studies at ETH Zurich remarks, “by operating in allied networks, Cyber Command is running the risk of causing the wrong type of friction,” eroding allied trust in the United States.<sup>17</sup> Those nations will surely often be no happier with this policy than many in the United States government would be if French cyber warriors took down Russian targets in Wisconsin. Just because the US military sees itself as liberating other nations’ computers from adversary occupation does not mean cyber GIs will be greeted with open arms.

Perhaps, in more normal times, partners might trust US intentions. But even the closest and most trusted US allies are feeling antagonized by recent decisions and actions of the United States. Extraterritorial US cyber operations may be perceived as just more bullying, to be resisted even if the outcome is beneficial. Smeets’s suggestion for “memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory” is a step in the right direction.<sup>18</sup>

US technology companies will be key partners to securing cyberspace but have not forgotten the revelations of Edward Snowden. “As story after story emerged alleging that the NSA undermined encryption, hacked into cables carrying the data of U.S. companies, placed implants and beacons in servers and routers, and generally weakened Internet security,” observes cybersecurity expert Adam Segal, “policymakers failed to comprehend the depth of Silicon Valley’s anger.”<sup>19</sup> If another Snowden-type revelation explodes, or more US military cyber weapons get stolen or leaked, the public-private partnerships called for in the strategy may disintegrate.<sup>20</sup>

### **Robust Interagency Process**

The latest National Cyber Strategy states that the US will use “diplomatic, information, military, . . . financial, intelligence, public attribution, and law enforcement capabilities” to counter malicious cyber activity—coordination that is especially needed to send clear signals and reassure partners.<sup>21</sup>

Shaping adversary behavior and improving stability require synchronized policy and operations across at least the National Security Council; Office of the Director of National Intelligence; Federal Bureau of Investigation; and Departments of State, Justice, Treasury, and Homeland Security. Coordinating these agencies has never been an easy task, yet the White House eliminated the cyber security coordinator position

in May 2018, and the Trump administration is already on its fourth national security advisor.<sup>22</sup>

## **Conclusion**

Offensive cyber operations can lead to “significant strategic advantages” for states, both the United States and its adversaries.<sup>23</sup> Persistent engagement may be the best chance to reduce conflict and return to a more secure cyberspace. But too many of the required elements are lacking to feel particularly confident.


Though the United States has strong military leadership and is building an effective cyber force, there are shortcomings in signaling to adversaries, building trust with partners, and establishing interagency coordination. Unfortunately, we cannot simply wish this were different or ignore the domestic and international political context.

Optimists and hawks may argue that having perhaps two of the five required elements is “good enough.” Some of the five elements could be merely preferable rather than strictly necessary, and these days even a weakly implemented strategy may be better than the alternatives. Incomplete advancement might still lead to significant national security gains or strategically delay adversaries long enough for the United States to develop the missing elements.

Pessimists will fear that persistent engagement might instead be like jumping a motorcycle across the Grand Canyon. Clearing two-fifths of the gap is a heroic feat but failure nonetheless—and may not be worth attempting without a greater chance of success. Defending forward could prompt adversaries to attack more, not less; international allies might see the United States as an adversary and not a partner; and US citizens and technology companies may believe that the US government cares more about taking the fight to the enemy than securing cyberspace, digital rights, or online privacy.

Persistent engagement may only be successful when used sparingly at the margins during a time of relative peace, when the effects on adversary operations, allies, and partners are easily overlooked. However, it may engender a harsher reaction when executed at scale—the main effort of a public and seemingly offensive strategy—or during a significant geopolitical crisis.

These issues might have been addressed when the strategy was still just an excellent idea rather than after its launch as the heart of a major military strategy. Now, government and military officials must shift attention to the lagging elements and, with researchers, track the effects of

the strategy to see if it is indeed stabilizing or inducing adversaries to step up their attacks.<sup>24</sup> 

**Jason Healey**

Senior Research Scholar  
School of International and Public Affairs  
Columbia University

**Stuart Caudill**

Master's Candidate  
Columbia University

**Notes**

1. Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 5, <https://doi.org/10.1093/cybsec/tyz008>.

2. Department of Defense, *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, September 2018), 4, <https://media.defense.gov/>.

3. US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: US Cyber Command, April 2018), 6, <https://www.cybercom.mil/>.

4. Ellen Nakashima, "Incoming NSA Chief Has a Reputation for Winning 'All the Important Fights.' Russia Will Be His Biggest Test Yet," *The Washington Post*, 1 April 2018, <https://www.washingtonpost.com/>.

5. United States Senate, Committee on Armed Services, "Hearing to Consider the Nomination of: General Mark A. Milley, USA, for Reappointment to the Grade of General and to Be Chairman of the Joint Chiefs of Staff," 11 July 2019, transcript, 116th Cong., 1st sess., 64, <https://www.armed-services.senate.gov/>.

6. US Cyber Command Public Affairs, "Cyber Mission Force Achieves Full Operational Capability," 17 May 2018, <https://www.cybercom.mil/>.

7. Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, 26 September 2019, <https://www.npr.org/>; and Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, 26 February 2019, <https://www.nytimes.com/>.

8. Government Accountability Office, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, DC: Government Accountability Office, March 2019), 17, <https://www.gao.gov/>.

9. Michael Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (blog), 9 November 2018, <https://www.lawfareblog.com/>.

10. For example, see Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017): 452–81; and Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

11. Chris Inglis, "Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, eds. Herbert Lin and Amy B. Zegart (Washington, DC: The Brookings Institution, 2018), 32.



12. Sean Gallagher, "US, Russia to Install 'Cyber-Hotline' to Prevent Accidental Cyberwar," *Ars Technica*, 18 June 2013, <https://arstechnica.com/>
13. Borghard and Loneragan, "The Logic of Coercion in Cyberspace," 471.
14. Department of Defense, *Summary: Department of Defense Cyber Strategy*, 1.
15. Eric Geller, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand," *POLITICO*, 16 August 2018, <https://politi.co/2MSWCnS>.
16. Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," 5.
17. Max Smeets, "Cyber Command's Strategy Risks Friction with Allies," *Lawfare* (blog), 28 May 2019, <https://www.lawfareblog.com/>.
18. Max Smeets, "NATO Allies Need to Come to Terms with Offensive Cyber Operations," *Lawfare* (blog), 14 October 2019, <https://www.lawfareblog.com/>.
19. Adam Segal, "The Internet Is Undermining America's Power," *Time*, 22 February 2016, <https://time.com/>.
20. Dan Goodin, "Stolen NSA Hacking Tools Were Used in the Wild 14 Months before Shadow Brokers Leak," *Ars Technica*, 7 May 2019, <https://arstechnica.com/>.
21. The White House, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 21, <https://www.whitehouse.gov/>.
22. Nicole Perlroth and David E. Sanger, "White House Eliminates Cybersecurity Coordinator Role," *The New York Times*, 15 May 2018, <https://www.nytimes.com/>.
23. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 105, <https://www.airuniversity.af.edu/>.
24. Jason Healey and Neil Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence Is Working or Failing," in *11th International Conference on Cyber Conflict: Silent Battle*, eds. T. Minarik et al. (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2019), 1–20, <https://ccdcoe.org/>.

# Artificial Intelligence: A Threat to Strategic Stability

JAMES S. JOHNSON

## Abstract

AI-augmented conventional capabilities might affect strategic stability between great military powers. The nuanced, multifaceted possible intersections of this emerging technology with a range of advanced conventional weapons can compromise nuclear capabilities, thus amplifying the potentially destabilizing effects of these weapons. This article argues that a new generation of artificial intelligence-enhanced conventional capabilities will exacerbate the risk of inadvertent escalation caused by the commingling of nuclear and nonnuclear weapons. The increasing speed of warfare will also undermine strategic stability and increase the risk of nuclear confrontation.

\*\*\*\*\*

The hyperbole surrounding artificial intelligence (AI) makes it easy to overstate the opportunities and understate the challenges posed by the development and deployment of AI in the military sphere.<sup>1</sup> Commingling and entangling nuclear and nonnuclear capabilities and the increasing speed of warfare may well undermine strategic stability.<sup>2</sup> From what we know today about emerging technology, new iterations of AI-augmented advanced conventional capabilities will compound the risk of military escalation,<sup>3</sup> especially inadvertent and accidental escalation.<sup>4</sup> While the potential escalation risks posed by advances in military technology have been discussed lightly in the literature, the potential of military AI to compound the risk and spark inadvertent escalation is missing.<sup>5</sup> This article addresses *how* and *why* AI could affect strategic stability between nuclear-armed great powers (especially China and the United States) and the multifaceted possible intersections of this disruptive technology with advanced conventional capabilities.<sup>6</sup>

Toward this end, the article conceptualizes and defines military-use AI and identifies a broad portfolio of nonnuclear weapons with “strategic effects”<sup>7</sup> along with their attendant enabling systems, including specific AI innovations that pose the greatest risks to nuclear stability.<sup>8</sup> Rather than provide a net assessment of all of the possible ways AI could influence

strategic stability, the article instead examines the possible stability enhancing and destabilizing effects in the nuclear domain using two examples: swarming autonomous weapon systems (AWS) and hypersonic weapons.<sup>9</sup>

### **Conceptualizing Military Artificial Intelligence**

Four core themes help conceptualize military-relevant AI.<sup>10</sup> First, AI does not exist in a vacuum. That is, in isolation AI will unlikely be a strategic game changer. Instead, it will mutually reinforce the destabilizing effects of existing advanced capabilities, thereby increasing the speed of warfare and compressing the decision-making time frame. Second, AI's impact on stability, deterrence, and escalation will likely be determined as much by a state's perception of its functionality than what it is capable of doing. In the case of nuclear policy, deterrence, and strategic calculations more broadly, the perception of an adversary's capabilities and intentions is as important as its actual capability. In addition to the importance of military force postures, capabilities, and doctrine, the effects of AI will therefore also have a strong cognitive element, increasing the risk of inadvertent escalation as a result of misperception and misunderstanding. For the foreseeable future, military AI will include a fair degree of human agency, especially in the safety-critical nuclear domain. Thus, strategic calculations on the use of force made in collaboration with machines at various levels will continue to be informed and shaped by human perceptions.

Third, the increasingly competitive and contested nuclear multipolar world order will compound the destabilizing effects of AI and, in turn, increase escalation risks in future warfare between great military powers—especially China and the United States. Moreover, the potential operational and strategic advantages offered by AI-augmented capabilities could prove irresistible to nuclear-armed strategic rivals. Thus motivated, adversaries could eschew the limitations of AI, compromising safety and verification standards to protect or attempt to capture technological superiority on the future digitized battlefield.<sup>11</sup> Finally, and related, against this inopportune geopolitical backdrop, the perceived strategic benefits of AI-powered weapons will likely attract states as a means to sustain or capture the technological upper hand over rivals. The most pressing risk posed to nuclear security is, therefore, the premature adoption of unsafe, error-prone, unverified, and unreliable AI technology in the context of nuclear weapons, which could have catastrophic implications.<sup>12</sup>

Military AI applications can be broadly categorized into those that have utility at a predominately operational or strategic level of warfare.<sup>13</sup> At the operational level, applications include autonomy<sup>14</sup> and robotics

(especially drone swarming); multi-actor interaction during red teaming and war gaming; big data-driven modeling;<sup>15</sup> and intelligence analysis to locate and monitor mobile missiles, submarines, mines, and troops movement.<sup>16</sup> At a strategic level, applications include (1) intelligence, surveillance, and reconnaissance (ISR) and command, control, communications, and intelligence (C3I) systems (especially in complex, adversarial, and cluttered environments);<sup>17</sup> (2) enhanced missile defense with machine-learning-augmented automatic target recognition (ATR) technology (i.e., improving target acquisition, tracking, guidance systems, and discrimination);<sup>18</sup> conventional precision missile munitions (including but not limited to hypersonic variants) able to target strategic weapons; (3) increased speed and scope of the observation, orientation, decision, and action (OODA) loop decision-making to augment air defense and electronic warfare (especially in antiaccess/area-denial [A2/AD] environments); and (4) AI-enhanced offensive and defensive cyber capabilities (e.g., machine learning techniques to infiltrate and uncover network vulnerabilities and to manipulate, spoof, and even destroy these networks).<sup>19</sup>

While the potential strategic effects of military AI are not unique or exclusive to this technology, the confluence of several trends weighs heavily on the pessimistic side of the instability-stability ledger: the rapid technological advancements and diffusion of military AI; the inherently destabilizing characteristics of AI technology (especially heightened speed of warfare, explainability, and vulnerability to cyberattack); the multifaceted possible intersections of AI with nuclear weapons; the interplay of these intersections with strategic nonnuclear capabilities; and the backdrop of a competitive multipolar nuclear world order, which may entice states to prematurely deploy unverified, unreliable, and unsafe AI-augmented weapons into combat situations. The historical record demonstrates that security competition—motivated by the desire to control warfare—tends to be ratcheted up because of the complexity of military technology and operations over time.<sup>20</sup> As a result, the Clausewitzian conditions of “fog and friction” will likely become a ubiquitous outcome of the uncertainties created by increasingly complex and inherently escalatory technologies.

From this perspective, the acceleration of modern warfare, the shortening of the decision-making time frame, and the commingling of military systems have occurred within the broader context of the computer revolution (e.g., remote sensing, data processing, acoustic sensors, communications, and cyber capabilities).<sup>21</sup> These overarching trends do *not* rely on AI and would have likely occurred whether AI were involved or not. AI is best understood, therefore, as a potentially powerful force mul-

tiplier of these developments. Put another way, military AI, and the advanced capabilities it enables, is a natural manifestation—rather than the cause or origin—of an established trend, potentially leading states to adopt destabilizing launch postures due to the increasing speed of war and commingling.<sup>22</sup>

The following three case studies ground the discussion of the core themes related to AI and the risk of inadvertent escalation to illustrate how and why military AI applications fused with nonnuclear weapons might cause or exacerbate escalation risks in future warfare. They also illuminate how these AI-augmented capabilities would work and, despite the risks associated with the deployment of these systems, why militaries might deploy them nonetheless. Because military commanders are concerned with tightly controlling the rungs on the “escalation ladder,” they should, in theory, be against delegating too much decision-making authority to machines—especially involving nuclear weapons.<sup>23</sup> Competitive pressures between great military powers and fear that others will gain the upper hand in the development and deployment of military AI (and the advanced weapon systems AI could empower) might overwhelm these concerns, however. By way of a caveat, the cases do not assume that militaries will necessarily be able to implement these augmented weapon systems in the near term. Disagreements exist among AI researchers and analysts about the significant operational challenges faced by states in the deployment of AI-augmented weapon systems.

### **Autonomous Weapons, Swarming, and Instability**

The proliferation of a broad range of AI-augmented autonomous weapon systems (most notably drones used in swarming tactics) could have far-reaching strategic implications for nuclear security and escalation in future warfare.<sup>24</sup> Several observers anticipate that sophisticated AI-augmented AWSs will soon be deployed for a range of ISR and strike missions.<sup>25</sup> Even if AWSs are used only for conventional operations, their proliferation could nonetheless have destabilizing implications and increase the risk of inadvertent nuclear escalation. For example, AI-augmented drone swarms may be used in offensive sorties targeting ground-based air defenses and by nuclear-armed states to defend their strategic assets (i.e., launch facilities and their attendant C3I and early-warning systems), exerting pressure on a weaker nuclear-armed state to respond with nuclear weapons in a use-them-or-lose-them situation.

Recent advances in AI and autonomy have substantially increased the perceived operational value that military great powers attach to the

development of a range of AWSs,<sup>26</sup> potentially making the delegation of lethal authority to AWSs an increasingly irresistible and destabilizing prospect.<sup>27</sup> That is, in an effort to defend or capture the technological upper hand in the possession of cutting-edge war-fighting assets vis-à-vis strategic rivals' traditionally conservative militaries, states may eschew the potential risks of deploying unreliable, unverified, and unsafe AWS. Today, the main risk for stability and escalation is the technical limitations of the current iteration of AI machine learning software (i.e., brittleness, explainability, unpredictability of machine learning, vulnerability to subversion or "data poisoning," and the fallibility of AI systems to biases).<sup>28</sup> To be sure, immature deployments of these nascent systems in a nuclear context would have severe consequences.<sup>29</sup>

Conceptually speaking, autonomous systems will incorporate AI technologies such as visual perception, speech, facial recognition, and decision-making tools to execute a range of core air interdiction, amphibious ground assaults, long-range strike, and maritime operations independent of human intervention and supervision.<sup>30</sup> Currently, only a few weapon systems select and engage their targets without human intervention. Loitering attack munitions (LAM)—also known as "loitering munitions" or "suicide drones"—pursue targets (such as enemy radars, ships, or tanks) based on preprogrammed targeting criteria and launch an attack when their sensors detect an enemy's air defense radar.<sup>31</sup> Compared to cruise missiles (designed to fulfill a similar function), LAMs use AI technology to shoot down incoming projectiles faster than a human operator ever could and can remain in flight (or loiter) for much longer periods. This attribute could complicate the ability of states to reliably and accurately detect and attribute autonomous attacks.<sup>32</sup>

A low-cost lone-wolf unmanned aerial vehicle (UAV) would, for example, not pose a significant threat to a US F-35 stealth fighter, but hundreds of AI machine learning autonomous drones in a swarming sortie may potentially evade and overwhelm an adversary's sophisticated defense capabilities—even in heavily defended regions such as China's east and coastal regions.<sup>33</sup> Moreover, stealth variants of these systems<sup>34</sup>—coupled with miniaturized electromagnetic jammers and cyberweapons—may be used to interfere with or subvert an adversary's targeting sensors and communications systems, undermining its multilayered air defenses in preparation for drone swarms and long-range stealth bomber offensive attacks.<sup>35</sup> In 2011, for example, MQ-1 and MQ-9 drones in the Middle East were infected with hard-to-remove malicious malware, exposing the vulnerability of US subset systems to offensive cyber.<sup>36</sup> This threat might,

however, be countered (or mitigated) by the integration of future iterations of AI technology into stealth fighters such as the F-35.<sup>37</sup> Manned F-35 fighters will soon be able to leverage AI to control small drone swarms in close proximity to the aircraft performing sensing, reconnaissance, and targeting functions, including countermeasures against swarm attacks.<sup>38</sup> In the future, extended endurance of UAVs and support platforms could potentially increase the ability of drone swarms to survive these kinds of countermeasures.<sup>39</sup>

Several prominent researchers have opined that, notwithstanding the remaining technical challenges as well as the legal and ethical feasibility,<sup>40</sup> we can expect to see operational AWSs in a matter of years.<sup>41</sup> According to former US deputy secretary of defense Robert Work, the United States “will not delegate lethal authority to a machine to make a decision” in the use of military force.<sup>42</sup> Work adds, however, that such self-restraint could be tested if a strategic competitor (especially China and Russia) “is more willing to *delegate authority* to machines than we are and, as that competition unfolds, we’ll have to make decisions on how we can best compete” (emphasis added).<sup>43</sup> In short, pre-delegating authority to machines, and taking human judgment further out of the crisis decision-making process, might severely challenge the safety, resilience, and credibility of nuclear weapons in future warfare.<sup>44</sup>

The historical record is replete with examples of near nuclear misses, demonstrating the importance of human judgment in mitigating the risk of miscalculation and misperception (i.e., of another’s intentions, redlines, and willingness to use force) between adversaries during crises.<sup>45</sup> Despite these historical precedents, the risks associated with unpredictable AI-augmented autonomous systems operating in dynamic, complex, and possibly a priori unknown environments remain underappreciated by global defense communities.<sup>46</sup> Eschewing these risks, China and Russia plan to incorporate AI into unmanned aerial and undersea vehicles for swarming missions infused with AI machine learning technology.<sup>47</sup> Chinese strategists have reportedly researched data-link technologies for “bee swarm” UAVs, particularly emphasizing network architecture, navigation, and anti-jamming military operations for targeting US aircraft carriers.<sup>48</sup>

Drones used in swarms are *conceptually* well suited to conduct preemptive attacks and nuclear ISR missions against an adversary’s nuclear and nonnuclear mobile missile launchers and nuclear-powered ballistic missile submarines (SSBN), along with their attendant enabling facilities (e.g., C3I and early warning systems, antennas, sensors, and air intakes).<sup>49</sup> The Defense Advanced Research Projects Agency (DARPA), for example, is

developing an autonomous surface vehicle (ASV) double outrigger, Sea Hunter, currently being tested by the US Navy to support antisubmarine warfare operations (i.e., submarine reconnaissance).<sup>50</sup> Some observers have posited that autonomous systems like Sea Hunter may render the underwater domain transparent, thereby eroding the second-strike deterrence utility of stealthy SSBNs. The technical feasibility of this hypothesis is highly contested, however.<sup>51</sup>

On the one hand, several experts argue that deployed in large swarms, these platforms could transform antisubmarine warfare, rendering at-sea nuclear deterrence vulnerable. On the other hand, some consider such a hypothesis technically premature because (1) it is unlikely that sensors on board AWSs would be able to reliably detect deeply submerged submarines; (2) the range of these sensors (and the drones themselves) would be limited by battery power over extended ranges;<sup>52</sup> and (3) given the vast areas traversed by SSBNs on deterrence missions, the chance of detection is negligible even if large numbers of autonomous swarms were deployed.<sup>53</sup> Thus, significant advances in power, sensor technology, and communications would be needed before these autonomous systems have a game-changing strategic impact on deterrence.<sup>54</sup> However, irrespective of the veracity of this emerging capability, the *mere perception* that nuclear capabilities face new strategic challenges would nonetheless elicit distrust between nuclear-armed adversaries—particularly where strategic force asymmetries exist. Moreover, DARPA's Sea Hunter demonstrates how the emerging generation of autonomous weapons is expediting the completion of the iterative targeting cycle to support joint operations, thus increasing the uncertainty about the reliability and survivability of states' nuclear second-strike capability and potentially triggering use-them-or-lose-them situations.

Conceptually speaking, the most destabilizing impact of AI on nuclear deterrence would be the synthesis of autonomy with a range of machine-learning-augmented sensors, undermining states' confidence in the survival of their second-strike capabilities and in extremis triggering a retaliatory first strike.<sup>55</sup> Enhanced by the exponential growth in computing performance and coupled with advances in machine learning techniques that can rapidly process data in real time, AI will empower drone swarms to perform increasingly complex missions, such as hunting hitherto hidden nuclear deterrence forces.<sup>56</sup> In short, the ability of future iterations of AI able to predict based on the fusion of expanded and dispersed data sets and then to locate, track, and target strategic missiles such as mobile



ICBM launchers in underground silos, on board stealth aircraft, and in SSBNs is set to grow.<sup>57</sup>

The following four scenarios illustrate the possible strategic operations AI-augmented drone swarms would execute.<sup>58</sup> First, drone swarms could be deployed to conduct nuclear ISR operations to locate and track dispersed (nuclear and nonnuclear) mobile missile launchers and their attendant enabling C3I systems.<sup>59</sup> Specifically, swarms incorporating AI-infused ISR, autonomous sensor platforms, ATR, and data analysis systems may enhance the effectiveness and speed of sensor drones to locate mobile missiles and evade enemy defenses.

Second, swarming could enhance legacy conventional and nuclear weapons delivery systems (e.g., ICBMs and SLBMs), possibly incorporating hypersonic variants (discussed below).<sup>60</sup> AI applications will likely enhance the delivery system targeting and tracking and improve the survivability of drone swarms against the current generation of missile defenses.

Third, swarming tactics could bolster a state's ability to disable or suppress an adversary's defenses (e.g., air, missile, and antisubmarine warfare defenses), clearing the path for a disarming attack.<sup>61</sup> Drone swarms might be armed with cyber or EW capabilities (in addition to antiship, anti-radiation, or regular cruise and ballistic missiles) to interfere with or destroy an adversary's early warning detection and C3I systems in advance of a broader offensive campaign.<sup>62</sup> Conversely, drone swarms might enhance states' missile defenses as countervails to these offensive threats. For example, swarms could form a defensive wall to absorb incoming missile salvos, intercepting them or acting as decoys to throw them off course with mounted laser technology.<sup>63</sup>

Finally, in the maritime domain, unmanned underwater vessels (UUV), unmanned surface vessels (USV), and UAVs supported by AI-enabled intra-swarm communication and ISR systems could be deployed simultaneously in both offensive and defensive antisubmarine warfare operations to saturate an enemy's defenses and to locate, disable, and destroy its nuclear-armed or nonnuclear attack submarines.<sup>64</sup> Despite continued advances in sensor technology design (e.g., reduced size and extended detection ranges) to overcome quieting challenges, other technical challenges still remain. These include communicating underwater between multiple systems, processing power requirements, generating battery life and energy, and scaling the system.<sup>65</sup>

While some experts do not expect a technically reliable and effective capability of this kind will be operational for at least a decade, others are more optimistic.<sup>66</sup> From a tactical perspective, drone swarms would not

need ocean-wide coverage (or full ocean transparency) to effectively detect and track submarines. According to UK rear admiral John Gower, a relatively even spread of sensors might be sufficient to enable “a *viable search and detection plan* . . . conceived for the open ocean” (emphasis added).<sup>67</sup> Moreover, advances in mobile sensing platforms could enable drones in swarms to locate submarines through chokepoints (or gateways) as they emerge from ports. Due to the current slowness of drones with extended sea ranges, however, trailing them autonomously seems implausible.<sup>68</sup> Future iterations of machine-learning-augmented UUVs and USVs may eventually complement, and perhaps replace entirely, the traditional role of general-purpose nuclear-powered submarines (SSN) and manned surface vehicles in tracking and trailing submarines of adversaries at chokepoints while simultaneously mounting sparsely distributed and mobile distributed network systems (DNS) sensors on UUVs.<sup>69</sup>

If a state views the credibility of its survivable nuclear weapons (especially nuclear-armed submarines) to be at risk,<sup>70</sup> conventional capabilities such as drone swarms will likely have a destabilizing effect at a strategic level.<sup>71</sup> Thus, even if swarm sorties were not intended as (or indeed technically capable of) a disarming first strike, the perception alone of the feasibility of such an operation would be destabilizing nonetheless. Moreover, the speed of AI could put the defender at a distinct disadvantage, creating additional incentives to strike first (or preemptively) technologically superior military rivals. Consequently, the less secure a nation considers its second-strike capabilities to be, the more likely it is to countenance the use of autonomous systems within its nuclear weapons complex to bolster the survivability of its strategic forces. According to analyst Paul Scharre, “winning in swarm combat may depend upon having the best algorithms to enable better coordination and *faster reaction times*, rather than simply the best platforms” (emphasis added).<sup>72</sup>

Combining speed, persistence, scope, coordination, and battlefield mass, AWSs will offer states attractive asymmetric options to project military power within contested A2/AD zones.<sup>73</sup> Enhanced by sophisticated machine learning neural networks, China’s manned and unmanned drone teaming operations could potentially impede future US freedom of navigation operations in the South China Seas.<sup>74</sup> Its air- and sea-based drones linked to sophisticated neural networks could, for example, support the People’s Liberation Army’s manned and unmanned teaming operations. Were China to infuse its cruise missiles and hypersonic glide capabilities with AI and autonomy, close-range encounters in the Taiwan Straits and the East and South China Seas would become more complicated, accident-

prone, and destabilizing—at both a conventional and nuclear level.<sup>75</sup> China is reportedly developing and deploying UUVs to bolster its underwater monitoring and antisubmarine capabilities as part of a broader goal to establish an “underwater Great Wall” to challenge US undersea military primacy. US AI-enhanced UUVs could, for example, theoretically threaten China’s nuclear ballistic and nonnuclear attack submarines.<sup>76</sup>

The deployment of new military technology in the nuclear domain, therefore, affects states differently depending on the relative strength of their strategic force structure. Thus, even if US UUVs were programmed only to threaten China’s nonnuclear attack fleets, Chinese commanders might nonetheless fear that their country’s nascent and relatively small—compared to US and Russian SSBN fleets—sea-based nuclear deterrent could be neutralized more easily.<sup>77</sup> Moreover, advances in machine learning sensor technology for enabling more accurate detection of Chinese SSBNs would likely reinforce Beijing’s concerns that it was being targeted by a militarily superior power—especially the United States. To test the veracity of this scenario, a better understanding of Chinese thinking on the utility of its nuclear and nonnuclear capabilities—and how it could inform China’s attitude to escalation risk—would be required.

Perceived as a relatively low-risk force majeure with ambiguous rules of engagement, and absent a robust normative and legal framework, autonomous weapons will likely become an increasingly attractive asymmetric to erode a militarily superior adversary’s deterrence and resolve.<sup>78</sup> In sum, notwithstanding the remaining technical challenges (especially the demand for power), swarms of robotic systems fused with AI machine learning techniques may presage a powerful interplay of increased range, accuracy, mass, coordination, intelligence, and speed in a future conflict.<sup>79</sup>

## **Hypersonic Boost-Glide Technology and Missile Defense**

Multiple advanced nonnuclear weapons could potentially threaten a wide range of strategic targets. In particular, technological advances in hypersonic boost-glide weapons—especially deployed in conjunction with cruise missiles, missile defense capabilities, and drone swarm support—could target an adversary’s high-value assets such as radars, antisatellite weapons, mobile missile launchers, C3I systems, and transporter-erector-launchers (TEL) used to undergird both nuclear and conventional missiles. In the future, swarms of AI-augmented UAVs could be used to locate and track dispersed targets such as mobile missile launchers and suppress enemy air defenses, clearing the path for swarms of hypersonic autonomous delivery systems armed with conventional or nuclear payloads.<sup>80</sup> The

development and deployment of offensive-dominant weapons such as hypersonic boost-glide weapons,<sup>81</sup> capable of threatening dual-use targets, could eventually exacerbate the problem of target ambiguity, increase the risks of inadvertent escalation, and, in turn, lower the nuclear threshold.<sup>82</sup>

It is noteworthy that Chinese, US, and Russian doctrinal texts share a common view of the potential utility of conventional hypersonic weapons to put at risk targets that hitherto only nuclear weapons could threaten, thereby bolstering strategic deterrence.<sup>83</sup> Moreover, in a future conflict between the US and China or the US and Russia, all sides would have strong incentives to attack the others' dual-use C3I and ISR capabilities early on and preemptively.<sup>84</sup> Chinese analysts view hypersonic cruise missiles, for example, as an effective means to enhance China's nuclear deterrence posture, penetrate US missile defenses, and preempt hypersonic (notably the X-37 unmanned spacecraft) scenarios.<sup>85</sup>

The maneuverability of hypersonic weapons could compound these dynamics, adding destination ambiguity to the destabilizing mix. In contrast to ballistic missiles, the unpredictable trajectories of hypersonic weapons will make using this weapon for signaling intent highly problematic and potentially escalatory. Furthermore, the challenge of determining an attacker's intentions would be complicated if an adversary's dual-use ISR, early warning, or C3I systems were targeted early on in a conflict. Adversaries unable to ascertain the intended path or ultimate target of a bolt-from-the-blue hypersonic strike will likely assume the worst (i.e., it was in a use-it-or-lose-it situation), inadvertently escalating a situation intended initially only to signal intent. Against the backdrop of geopolitical competition and uncertainty, the reciprocal fear of surprise attack will likely heighten the risk of miscalculation, with potentially escalatory implications.<sup>86</sup>

For example, if China's early warning systems detected a hypersonic weapon launched from the US, Beijing would not be sure whether China was the intended target ("destination ambiguity"). Even if it became clear that China was the intended target, Beijing would still not know what assets the US intended to destroy ("target ambiguity") or whether the weapon was nuclear or conventionally armed ("warhead ambiguity"). China's AI-augmented—and likely dual-use—early warning systems would be a mixed blessing for strategic stability, however. Perhaps Beijing's confidence in the survivability of its nuclear forces could have a stabilizing effect. Then again, allowing China to detect an incoming weapon much earlier in a conflict might exacerbate warhead and target ambiguity, thus generating inadvertent escalatory risks. If China made improvements to its missile early warning system in preparation for the

adoption of a launch-under-attack nuclear posture (like Russia and the United States), then the early detection of a US boost-guide attack would become even more critical.<sup>87</sup>

According to analyst James Acton, enabling capabilities are critical for the successful employment of hypersonic weapons.<sup>88</sup> In particular, military operations that require rapid decision-making (i.e., to locate, track, and accurately execute an attack) will generally place higher demands on enabling capabilities to plan and execute a strike (especially ISR) than preemptive or surprise attacks. To date, however, command and control, ISR, intelligence collation and analysis, and battle damage assessment remain undeveloped, lagging the progress made in hypersonic weapon technology.<sup>89</sup> AI technology is expected to accelerate progress for hypersonic weapons and other long-range (conventional and nuclear-armed) precision munitions in all of these critical enabling capabilities:<sup>90</sup> (1) autonomous navigation and advanced vision-based guidance systems,<sup>91</sup> (2) ISR systems for targeting and tracking (especially mobile) targets, (3) missile release and sensor systems, (4) AI machine learning systems to decipher patterns from large data sets to support intelligence analysis for identifying and tracking targets,<sup>92</sup> (5) pattern interpretation to cue decision support systems for enabling “fire and forget” missiles,<sup>93</sup> and (6) escalation prediction.<sup>94</sup> For example, several states (notably China and Russia) are developing machine learning approaches to build control systems for hypersonic glide vehicles (HGV), which because of their high velocity cannot be operated manually.

These autonomous variants could also enhance hypersonic missile defenses, strengthening their resilience against countermeasures such as jamming and spoofing.<sup>95</sup> Conceptually, within a matter of minutes, AI machine learning systems can generate a hypersonic flight plan for human review and approval, and in real-time, self-correct a missile in flight to compensate for unexpected flight conditions or a change in the target’s location.<sup>96</sup> Theoretically, this AI augmentation would enable swarms of hypersonic autonomous delivery systems to circumvent some of the remaining technical challenges that militaries face in tracking and targeting an adversary’s mobile missile forces. Specifically, it would allow tracking a moving target and communicating this information back to commanders in real time, and then cueing a rapid surprise or preemptive attack *before* the mobile launchers can be relocated.<sup>97</sup>

A large volume of Chinese open sources reveals prolific indigenous research into the integration of AI-powered machine learning techniques, especially deep neural networks, to address the technical challenges

associated with the high-speed and heat-intensive reentry dynamics of hypersonic weapons (i.e., heat control, maneuverability, stability, and targeting).<sup>98</sup> Particularly, Chinese analysts anticipate that AI will resolve many of the intractable issues associated with hypersonic glide vehicles' high flight envelope, including complex flight environments, severe non-linearity, intense and rapid time variance, and the dynamic uncertainty during the dive phase of the delivery. They broadly concur with their Western counterparts that much like other AI-augmented strategic non-nuclear capabilities (i.e., drone swarms, cyber and EW capabilities, missile defense, and antisubmarine capabilities), hypersonic weapons—by increasing the speed of warfare—are inherently destabilizing.

Chinese efforts to apply AI machine learning techniques to enhance hypersonic weapons can be understood as part of a broader strategic goal of developing “intelligent” autonomous weapons, and their enabling systems, for the future multidimensional and multidomain battlefield environment.<sup>99</sup> Because of the many intersections AI-enhanced hypersonic weapons could have with nuclear security (especially the penetration of US missile defenses), together with the strong likelihood Chinese hypersonic weapons will carry dual payloads,<sup>100</sup> an appreciation of the interaction between these capabilities and implications for nuclear, conventional, and cross-domain deterrence will be a critical task for analysts and policy makers.<sup>101</sup> Similar to the cyber capabilities, AWSs, and other advanced automated weapon systems that AI could empower, hypersonic weapons could significantly accelerate the pace of conflict and compress the decision-making time frame. In sum, as a powerful enabler and force multiplier, AI could disrupt information flows and effective communication (both between adversaries and allies and within military organizations) and, consequently, complicate escalation management during future crisis or conflict—especially involving China and the United States.<sup>102</sup> Furthermore, the disruption of communications might also undermine nuclear deterrence and therefore increase the odds of brinkmanship and incentives to act first and preemptively during a crisis.

## **Conclusion**

A new generation of AI-augmented advanced conventional capabilities will exacerbate the risk of inadvertent escalation caused by the commingling of nuclear and strategic nonnuclear weapons (or conventional counterforce weapons) and the increasing speed of warfare, thereby undermining strategic stability and increasing the risk of nuclear confrontation. This conclusion is grounded in the overarching findings that relate to

*how* and *why* AI could affect strategic stability between great military powers—especially China and the United States.


If a state perceives that the survivability of its nuclear forces were at risk, advanced conventional capabilities (e.g., autonomous drone swarms and hypersonic weapons) augmented with AI machine learning techniques will have a destabilizing impact at a strategic level of conflict. AI's effect on strategic stability will likely be determined by states' perceptions of its operational utility rather than actual capability. If an adversary underestimates the potential threat posed by nascent and especially poorly conceptualized accident-prone autonomous systems, the consequences would be severely destabilizing.

Despite the speed, diverse data pools, and processing power of algorithms compared to humans, complex AI-augmented systems will still depend on the assumptions encoded into them by human engineers to simply extrapolate inferences—potentially erroneous or biased—from complexity, resulting in unintended outcomes. One of the most significant escalatory risks caused by AI is likely to be, therefore, the perceived pressure exerted on nuclear powers in the use of AI-augmented conventional capabilities to adopt unstable nuclear postures (such as launch on warning, rescinding no-first-use pledges, or nuclear war fighting), or even to exercise a preemptive first nuclear strike during a crisis. In extremis, human commanders might lose control of the outbreak, course, and termination of warfare.

Further, a competitive and contested multipolar nuclear environment will likely exacerbate the potentially destabilizing influence of AI, increasing that risk of inadvertent escalation to a nuclear level of conflict between great military powers. In today's multipolar geopolitical order, therefore, relatively low-risk and low-cost AI-augmented AWS capability—with ambiguous rules of engagement and absent a robust normative and legal framework—will become an increasingly enticing asymmetric option to erode an advanced military's deterrence and resolve. By disrupting effective and reliable flows of information and communication between adversaries and allies and within military organizations, AI-augmented conventional weapon systems (i.e., C3I, early warning systems, and ISR) could complicate escalation management during future crisis or conflict—especially involving China and the United States.

A prominent theme that runs through the scenarios in this article—and central to understanding the potential impact of AI for strategic stability and nuclear security—is the concern that AI systems operating at machine speed will push the pace of combat to a point where machine actions

surpass the cognitive and physical ability of human decision-makers to control or even comprehend events. Effective deterrence depends on the clear communication of credible threats and consequence of violation between adversaries, which assumes the sender and recipient of these signals share a common context allowing for mutual interpretation.<sup>103</sup>

For now, it remains axiomatic that human decisions escalate a situation; however, military technology like AI that enables offensive capabilities to operate at higher speed, range, and lethality will move a situation more quickly up the escalation rungs, crossing thresholds that can lead to a strategic level of conflict. These escalatory dynamics would be greatly amplified by the development and deployment of AI-augmented tools functioning at machine speed. Military AI could potentially push the pace of combat to a point where the actions of machines surpass the cognitive and physical ability of human decision-makers to control (or even fully understand) future warfare. Thus, until experts can unravel some of the unpredictable, brittle, inflexible, unexplainable features of AI, this technology will continue to outpace strategy, and human error and machine error will likely compound one another—with erratic and unintended effects. 

#### James S. Johnson

Dr. James Johnson is a postdoctoral research fellow at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies, Monterey. He holds a PhD in politics and international relations from the University of Leicester, where he is also an honorary visiting fellow with the School of History and International Relations. Dr. Johnson is fluent in Mandarin and has published widely in the fields of security and strategic studies, Sino-American security relations, nuclear nonproliferation and arms control, emerging technology (especially AI), Chinese foreign policy, and East Asian security. He is the author of *The US-China Military and Defense Relationship during the Obama Presidency* (Palgrave Macmillan, 2018). His latest book project is entitled *Artificial Intelligence and the Future of Warfare: USA, China, and Strategic Stability*.

#### Notes

1. Recent progress in AI falls into two distinct fields: (1) “narrow” AI and specifically machine learning and (2) “general” AI, which refers to AI with the scale and fluidity akin to the human brain. Narrow AI is already used in the private sector, particularly in data-rich research fields and applied sciences (e.g., predictive analytics for market research, consumer behavior, logistics, and quality control systems). The distinction between narrow and general AI might, however, be less of an absolute, or binary, measure than one of degree. Breakthroughs in narrow AI have generally led to speculation on the arrival of artificial general intelligence. Most experts agree, however, that the development of general AI is at least several decades away, if at all. Stuart Armstrong, Kaj Sotala, and Seán S. ÓÉigeartaigh, “The Errors, Insights and Lessons of Famous AI Predictions—and What They Mean for the Future,” *Journal of Experimental and Theoretical Artificial Intelligence* 26, no. 3 (2014): 317–42, DOI: 10.1080/0952813X.2014.895105.



2. “Entanglement” in this context refers to dual-use delivery systems that can be armed with nuclear and nonnuclear warheads; the commingling of nuclear and non-nuclear forces and their support structures; and nonnuclear threats to nuclear weapons and their associated command, control, communications, and intelligence (C3I) systems. “Strategic stability” as a concept in political science has been defined in many ways. Colby Elbridge and Michael Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, PA: Army War College, 2013), <https://publications.armywarcollege.edu/>.

3. Military-use AI, and the advanced capabilities it enables, can be conceptualized as a natural manifestation (rather than the cause or origin) of an established trend in emerging technology toward commingling and increasing the speed of warfare, which could lead states to adopt destabilizing launch postures. Hans M. Kristensen, Matthew McKinzie, and Theodore A. Postol, “How US Nuclear Force Modernization Is Undermining Strategic Stability: The Burst-Height Compensating Super-Fuze,” *Bulletin of the Atomic Scientists*, 1 March 2017, <https://thebulletin.org/>.

4. “Inadvertent escalation” refers to a situation where one state takes an action that it does not believe the other side will (or should) regard as escalatory but occurs *unintentionally* nonetheless. See Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1991); Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008), <https://www.rand.org/>; and Lawrence Freedman, *Evolution of Nuclear Strategy*, 3rd ed. (London: Palgrave Macmillan, 2003), especially chap. 14.

5. Notable exceptions include Vincent Boulanin, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. I, *Euro-Atlantic Perspectives* (Stockholm: SIPRI Publications, May 2019), <https://www.sipri.org/>; Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018), <https://www.rand.org/>; Kareem Ayoub and Kenneth Payne, “Strategy in the Age of Artificial Intelligence,” *Journal of Strategic Studies* 39, nos. 5–6 (2016): 793–819, DOI: 10.1080/01402390.2015.1088838; Technology for Global Security (T4GS) and the Center for Global Security Research (CGSR), “AI and the Military: Forever Altering Strategic Stability,” T4GS Reports, 13 February 2019, <https://www.tech4gs.org/>; Jürgen Altmann and Frank Sauer, “Autonomous Weapon Systems and Strategic Stability,” *Survival* 59, no. 5 (2017): 121–27, DOI: 10.1080/00396338.2017.1375263; and James S. Johnson, “Artificial Intelligence and Future Warfare: Implications for International Security,” *Defense and Security Analysis* 35, no. 2: 147–69, DOI: 10.1080/14751798.2019.1600800.

6. Thomas J. Christensen, “The Meaning of the Nuclear Evolution: China’s Strategic Modernization and U.S.-China Security Relations,” *Journal of Strategic Studies* 35, no. 4 (August 2012): 467–71; and Fiona S. Cunningham and M. Taylor Fravel, “Assuring Assured Retaliation: China’s Nuclear Posture and U.S.-China Strategic Stability,” *International Security* 40, no. 2 (Fall 2015): 40–45, <https://www.belfercenter.org/>.

7. Examples of strategic capabilities include kinetic long-range nuclear and conventional munitions (e.g., ICBMs), long-range penetrating bombers, and shorter-range tactical (or theater) weapons that are or can be forward deployed. A range of technologically advanced (offensive and defensive) nonnuclear (kinetic and nonkinetic) weapons designed to reduce the vulnerability of states to nuclear attack can also have strategic effects. For example, offensive cyber and counterspace (i.e., ASATs) have recently emerged as strategic capabilities. Defense systems (e.g., ballistic missile defense systems)

can also be viewed as strategic in as much as they are intended (or able) to impair the ability of a state to respond at a strategic level.

8. The author acknowledges that new military terms or concepts do not necessarily represent operational or deployable capabilities.

9. For the impact of AI and machine learning technology on the cyber (nonkinetic) domain, see James S. Johnson, "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence, and Strategic Stability," *Journal of Cyber Policy* 4, no. 3 (2019): 442–60, DOI: 10.1080/23738871.2019.1701693.

10. See James S. Johnson, "Artificial Intelligence and Future Warfare: Implications for International Security," *Defense and Security Analysis* 35, no. 2 (2019): 147–69, DOI: 10.1080/14751798.2019.1600800.

11. Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018), <https://www.rand.org/>; and Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," 799–819.

12. The DOD has long recognized these kinds of concerns. For example, the Air Force's Tacit Rainbow anti-radiation missile program, which incorporated elements of unmanned aerial vehicles (UAV) and cruise missiles, was canceled in 1991 in large part because of the risk of error posed by autonomous systems used in offensive missions.

13. The line between core AI and "AI-related" technology is a blurred one. For the purposes of this article, core AI technology includes machine learning (and deep learning and deep networks subset), modelling, automated language and image recognition, voice assistants, and analysis support systems. Also, AI-related (and AI-enabling) technology includes autonomous vehicles, big data analytics, 5G networks, supercomputers, smart vehicles, smart wearable devices, robotics, and the Internet of Things, to name a few.

14. "Autonomy" in the context of military applications can be defined as the condition or quality of being self-governing to achieve an assigned task based on a system's own situational awareness (integrated sensing, perceiving, and analyzing), planning, and decision-making. That is, autonomy is fundamentally a software endeavor. Software (i.e., AI machine learning techniques for sensing, modeling, and decision-making) rather than hardware separates existing armed unmanned and remote-controlled weapon systems (e.g., the US MQ-9 Reaper, the Israeli Guardium, and the Russian Platform-M). A distinction is often made between automatic, automated, and autonomous systems, although these terms are sometimes used interchangeably. For the purposes of this article, it is necessary to acknowledge that this debate exists. See Department of Defense Directive (DODD) 3000.09, *Autonomy in Weapon Systems*, 21 November 2012, <https://fas.org/>.

15. For example, AI is enabling scientists to model nuclear effects to confirm the reliability of nuclear stockpiles without nuclear testing.

16. For example, the US National Geospatial Intelligence Agency has reportedly used AI to support military and intelligence analysis.

17. A recent Stockholm International Peace Research Institute (SIPRI) report found that autonomy is used in at least 56 military systems to collect and process various types of information, especially related to targeting and command and control. Vincent Boulanin and Maaike Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm, Sweden: SIPRI, 2017), 28, <https://www.sipri.org/>.

18. Since the 1970s, air defense systems have been using an AI technology to augment automatic target recognition to detect, track, prioritize, and select incoming air threats.

19. Daniel S. Hoadley and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington, DC: Congressional Research Service, 2018), <https://kr.usembassy.gov/>.
20. Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977), <https://ratical.org/>.
21. Lieber A. Keir and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (2017): 9–49; and Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?," *Survival* 60, no. 5 (2018): 7–32, DOI: 10.1080/00396338.2018.1518374.
22. Kristensen, McKinzie, and Postol, "Nuclear Force Modernization."
23. Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).
24. Recent studies generally agree that AI machine learning systems are an essential ingredient to enable fully autonomous systems. See Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. (Harlow, Essex: Pearson Education, 2014), 56; and Michael Horowitz, Paul Scharre, and Alex Velez-Green, *A Stable Nuclear Future? The Impact of Automation, Autonomy, and Artificial Intelligence* (Philadelphia: University of Pennsylvania, 2017).
25. See Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Applications* (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015), <https://www.hsdl.org/>; Zachary Kallenborn and Philipp C. Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *The Nonproliferation Review* 25, nos. 5–6 (2018): 523–43, DOI: 10.1080/10736700.2018.1546902; and Bryan Clark, *The Emerging Era in Undersea Warfare* (Washington, DC: Center for Strategic and Budgetary Analysis, 2015), <https://csbaonline.org/>.
26. AI and autonomy—together with automatic and automated—are often used interchangeably. Autonomous systems are best understood as a key subset of AI technologies—especially machine learning.
27. To date, no state has formally declared an intention to build entirely autonomous weapon systems. Currently, only the United States, the United Kingdom, and Israel have used armed drones operationally.
28. Machine learning is a concept that encompasses a wide variety of techniques designed to identify patterns in and also "learn" and make predictions from data sets. Successful learning depends on having access to vast pools of reliable data about past behavior and successful outcomes. The "neural network" approach to AI represents only a small segment of the improvements in AI techniques. AI also includes, for example, language processing, knowledge representation, and inferential reasoning, which are being actualized by the rapid advancements in software, hardware, data collection, and data storage. Jürgen Schmidhuber, "Deep Learning in Neural Networks: An Overview," *Neural Networks* 61 (2015): 85–117, <http://www2.econ.iastate.edu/>.
29. Will Knight and Karen Hao, "Never Mind Killer Robots—Here Are Six Real AI Dangers to Watch out for in 2019," *MIT Technology Review*, 7 January 2019, <https://www.technologyreview.com/>.
30. The US DOD has developed directives restricting development and use of systems with particular autonomous capabilities; "humans" must be kept in the loop and directly make the decisions for all applications of lethal force.

31. LAMs are hybrid offensive capabilities between guided munitions and unmanned combat aerial systems. To date, the only known operational LAM is Israel's Harop (or Harpy 2), combining a human-in-the-loop and fully autonomous mode.

32. For example, the terrorist group ISIS used remotely controlled aerial drones in its military operations in Iraq and Syria. Ben Watson, "The Drones of ISIS," *Defense One*, 12 January 2017, <https://www.defenseone.com/>.

33. There are instances when a lone-wolf drone can pose a serious threat to an F-35; a single drone can destroy an F-35 on the ground. For example, an unmanned aerial system could be employed to place spike strips on a runway to deflate aircraft tires, deliver debris to damage jet engines, drop explosives on other targets, or even in a Kamikaze role during the critical takeoff or landing phases of flight, increasing the chances of damage or a catastrophic crash. Thomas S. Palmer and John P. Geis, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," *Air and Space Power Journal* 31, no. 2 (Summer 2017): 105, <https://www.airuniversity.af.edu/>.

34. China, the United States, the United Kingdom, and France have developed and tested stealthy UAV prototypes.

35. The Russian military, for example, reportedly deployed jammers to disrupt GPS-guided unmanned air vehicles in combat zones including Syria and Eastern Ukraine.

36. Noah Shachtman, "Computer Virus Hits US Drone Fleet," *Wired*, 7 October 2011, <https://www.wired.com/>

37. AI-infused algorithms able to integrate sensor information, consolidate targeting, automate maintenance, and merge navigation and sensor information are currently being developed and tested to anticipate the kinds of high-intensity future threat environments posed by drone swarming.

38. Currently, small drone technology does not enable drones to fly at speeds where they could be, or remain, in close proximity to the aircraft. Most existing concepts involve either medium-sized (e.g., MQ-9) drones acting as wingmen to a fighter jet (e.g., F-35), and thus in close proximity, or small drones released as a payload that does not remain in close proximity to the fighter, with little to no guidance from the mother ship. The author thanks the anonymous reviewer for making this point.

39. A combination of restrictions outlined in DODD 3000.09, *Autonomy in Weapons Systems*, as well as the cultural and bureaucratic norms and practices in the US armed services, will likely stymie efforts to incorporate AI-enabled systems. This will particularly apply in situations where the demand increases for manpower skilled in fields such as computer science (especially AI machine learning), engineering, and the sciences.

40. While recent breakthroughs in AI have made possible the automation of several tasks previously considered complex (e.g., dependable vehicle control and air traffic control), there remain technical limits on what computers and robots can achieve autonomously. Boulanin, *Impact of Artificial Intelligence*, vol. 1, chap. 3.

41. The moral and ethical considerations related to the use of autonomous control weapons and autonomous targeting are complex and highly contested; humans creating technology to attack a human is inherently problematic.

42. "WATCH: David Ignatius and Pentagon's Robert Work on the Latest Tools in Defense," *Washington Post Live* (blog), 30 March 2016, <https://www.washingtonpost.com/>.

43. "WATCH: David Ignatius and Pentagon's Robert Work," video. Kalashnikov, a Russian defense contractor, has reportedly built an unmanned ground vehicle (the

Soratrik) and plans to develop a broad range of autonomous systems infused with sophisticated AI machine learning algorithms.

44. UAVs used in swarming operations do not necessarily need to be “fully autonomous”; humans could still decide to execute a lethal attack.

45. Patricia Lewis et al., *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Chatham House, Royal Institute of International Affairs, 2014), <https://www.chathamhouse.org/>.

46. Modeling interactions with other agents (especially humans) in either a competitive or a collaborative context is inherently problematic because human behavior is often unpredictable. Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), xv, <https://www.cna.org/>.

47. This Russian unmanned submarine is known by the Pentagon as “Kanyon”; its onboard nuclear warheads are considered capable of destroying ports and cities.

48. Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington, DC: Center for a New American Security, DC: November 2017), 23, <https://s3.amazonaws.com/>.

49. Currently, the types of airborne drones that militaries are considering using in swarms are small and thus limited in range. Supplying sufficient power for swarms of UAVs or unmanned underwater vessels (UUV) for extended periods would require significant improvements in battery technology, air-independent propulsion, or fuel-cell technology. Further, many states' nuclear-related facilities (except the SSBNs) are located well inland, which (for now) makes drones ill-suited to attack these targets unless lifted in by a different platform. Electric storage battery power capacity is, however, rapidly improving, and experts predict a tenfold increase in power and endurance within the next decade. Leslie F. Hauck and John P. Geis II, “Air Mines: Countering the Drone Threat to Aircraft,” *Air and Space Power Journal* 31, no. 1 (Spring 2017): 26–40, <https://www.airuniversity.af.edu/>.

50. Joseph Trevithick, “Navy's Sea Hunter Drone Ship Has Sailed Autonomously to Hawaii and Back amid Talk of New Roles,” *The Drive*, 4 February 2019, <https://www.thedrive.com/>.

51. While there are a number of technologies under development specifically designed to track SSBNs (e.g., the DOD's Sea Hunter, a prototype autonomous surface vehicle), these programs remain immature.

52. Unlike standard UUVs that are typically tethered and have a very short range, underwater gliders (e.g., US Liquid Robotics Wave Rider SV3), while slow, can roam over long distances for months at a time.

53. Jonathan Gates, “Is the SSBN Deterrent Vulnerable to Autonomous Drones?,” *The RUSI Journal* 161, no. 6 (2016): 28–35, DOI: 10.1080/03071847.2016.1265834.

54. Drones (including UAVs, UUVs, and unmanned surface vessels or USVs) might nonetheless have a significant qualitative impact on antisubmarine warfare. For example, drone swarms deployed to chokepoints (or gateways) or to an adversary's docking exit routes could act as a layered physical barrier, deterring or denying an opponent's submarine the ability to operate in certain military zones (i.e., A2/AD zones).

55. Given the current limits on drone range (i.e., battery power) and limited payload, it is unlikely that drone technology will mature sufficiently to represent a credible threat to states' nuclear assets (or other hardened targets) in the near term (i.e., within five

years)—unless, for example, UAVs are able to infiltrate hardened targets via an air duct or other like passage.

56. Tom Simonite, “Moore’s Law Is Dead. Now What?,” *MIT Technology Review*, 13 May 2016, <https://www.technologyreview.com/>. In addition to UAVs, emerging space technologies will soon enable drone-like surveillance from space incorporating similar machine learning techniques. Larger satellite constellations coupled with smaller individual satellites are expected to provide continuous coverage over large geographical ranges.

57. Elias Groll, “How AI Could Destabilize Nuclear Deterrence,” *Foreign Policy*, 24 April 2018, <https://foreignpolicy.com/>.

58. The value of AWSs in these scenarios does not mean that they are the only or necessarily most effective way to fulfill these missions. Gates, “Is the SSBN Deterrent Vulnerable?,” 28–35.

59. In 2011, students at the Massachusetts Institute of Technology presented the fully autonomous, fixed-wing Perdix UAV capable of between-drone communication at the 2011 Air Vehicle Survivability Workshop. In addition to the US, Russia, South Korea, and China are also actively pursuing drone swarm technology programs. Kallenborn and Bleek, “Swarming Destruction,” 1–2.

60. At least two nuclear-armed states are considering the possibility of using UAVs or UUVs for nuclear delivery. Russia, in 2015, revealed the development of a large nuclear-armed UUV, Poseidon (also known as Status-6). The US is also developing a nuclear-capable long-range bomber, the B-21 Raider, that could potentially be used to operate remotely while carrying nuclear payloads. Other unmanned combat aerial vehicle (UCAV) prototypes (e.g., Northrop Grumman X47B, the Dassault nEUROn, and the BAE Systems Taranis) could also feasibly be used in nuclear attacks. Boulanin, *Impact of Artificial Intelligence*, vol. 1, 56–57.

61. Mike Pietrucha, “The Need for SEAD Part 1: The Nature of SEAD,” *War on the Rocks*, 17 May 2016, <https://warontherocks.com/>.

62. Polat Cevik et al., “The Small and Silent Force Multiplier: A Swarm UAV-Electronic Attack,” *Journal of Intelligent and Robotic Systems* 70 (April 2013): 595–608, <https://doi.org/10.1007/s10846-012-9698-1>.

63. While the Missile Defense Agency (MDA) is developing lasers for drones, the size of a drone needed to power a laser of meaningful power would be very large. The likelihood, therefore, we will see lasers on drones in the near term is considered low. The MDA estimates that the first prototype laser for a fighter-sized platform will likely be completed in approximately two years. The US MDA recently requested a significant budget to develop a drone-mounted laser program. Jen Judson, “MDA Awards Contracts for a Drone-Based Laser Design,” *Defense News*, 11 December 2017, <https://www.defensenews.com/>.

64. The US Defense Advanced Research Projects Agency (DARPA) is currently developing an antisubmarine warfare continuous trail unmanned vehicle capability, the Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) program, to track quiet diesel-electric submarines with USVs from the surface.

65. Unmanned drone platforms are capable of carrying several types of sensors, and the swarming machine-learning systems to control them are either available today or in advanced stages of development. These sensors include active and passive sonar, magnetic anomaly detectors (MAD), light detection and ranging (LIDAR) for wake detection, thermal sensors, and laser-based optical sensors capable of piercing seawater.

66. Sebastian Brixey-Williams, “Will the Atlantic Become Transparent?,” 2nd ed., *British Pugwash*, November 2016, 2–6, <https://britishpugwash.org/>.

67. John Gower, “Concerning SSBN Vulnerability—Recent Papers,” British American Security Information Council (BASIC), *Analysis* (blog), 10 June 2016, <https://basicint.org/>.

68. It might be possible for a handoff to occur between drones in a grid to monitor a submarine as it moves, but doing so in extended ranges and duration would be cumbersome and slow.

69. To date, the US Navy has deployed and tested DNSs in littoral waters. For example, PLUSNet (persistent littoral undersea surveillance network) is a joint project between the US Navy’s Office of Naval Research (ONR) and DARPA that began in 2005.

70. Whether autonomous underwater vehicles involved in a future swarm attack on a nuclear-armed submarine were armed or programmed merely to track and monitor a submarine, the destabilizing effects on deterrence would likely be similar. Altmann and Sauer, “Autonomous Weapon Systems,” 131.

71. In an asymmetric encounter involving adversaries who do not possess AWS capabilities, the escalatory cycles described above would unlikely occur. Sauer, 132.

72. Paul Scharre, “Counter-Swarm: A Guide to Defeating Robotic Swarms,” *War on the Rocks*, 31 March 2015, <https://warontherocks.com/>.

73. China’s military has incorporated a range of advanced UAVs into all four services of its force structure.

74. In early 2018, China began construction of the world’s largest test site for unmanned UAVs for war and peacetime surveillance operations in the South China Sea. For example, the Haiyi (or “Sea Wing”) UUV glider has been used in several scientific missions in the South China Sea. “Sea Wing Series of Underwater Gliders Achieves the Largest Model of Swarms Simultaneously Observing,” Shenyang Institute of Automation, 24 August 2017.

75. Reports indicate that China is engaged in the development of several potentially destabilizing capabilities including research into the use of AI and autonomy in prompt and high-precision (cruise and ballistic) missile systems, space planes, and a variety of hypersonic boost-glide variants. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China, 2019* (Washington, DC: Department of Defense, 2019), <https://media.defense.gov/>.

76. A range of autonomous ground and underwater vehicles is already in development globally with varying degrees of success.

77. Chinese reports from the 2016 seizure of a US UUV indicate that this action was taken because of the perceived threat to Chinese SSBNs in the region.

78. Paul Scharre, *Autonomous Weapons and Operational Risk: Ethical Autonomy Project* (Washington, DC: Center for a New American Security, February 2016), <https://s3.amazonaws.com/>.

79. Supplying sufficient power for swarms of UAVs (or UUVs) for an extended period would require significant improvements in either battery technology, air-independent propulsion, or fuel cell technology. It may also require the development of some form of energy storage mechanism that has yet to be envisaged. Gates, “Is the SSBN Deterrent Vulnerable?,” 28–35.

80. Currently, ballistic missiles mounted with hypersonic boost-glide vehicles can only maneuver while inside the atmosphere, and the density of the atmosphere at the

turning point dictates their rate of turn. Tight turns are only possible near the ground and in close proximity to the target.

81. Russia, China, and the United States have been most active in the development of hypersonic weapons. To date, however, no state has emerged as the dominant leader in this nascent technology. James M. Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks* (Washington, DC: Carnegie Endowment for International Peace, 2017), 54, <https://carnegieendowment.org/>.

82. Currently, the drag associated with hypersonic glide vehicles remaining in the atmosphere will require new propulsion technologies and innovation in ablative materials to absorb the increased heat, both of which are not expected to emerge in the near term. The author would like to thank an anonymous reviewer for making this point.

83. A particular concern identified by Russian and Chinese analysts is the possibility that a combination of US ballistic missile defense and high-precision conventional weapons (such as hypersonic weapons) could permit the US to attempt a disarming first strike without crossing the nuclear Rubicon.

84. Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security* 37, no. 4 (2013): 67–68, <https://muse.jhu.edu/>.

85. This view in large part reflects a misperception held by Chinese analysts that the US's hypersonic and conventional prompt global strike programs are guided by clearly defined and coherent military (versus technological) objectives targeting China. As a result, Beijing would more likely perceive an ambiguous situation as an attack on its nuclear arsenals.

86. James Johnson, "The End of Military-Techno *Pax Americana*? Washington's Strategic Responses to Chinese AI-Enabled Military Technology," *The Pacific Review*, 2019, <https://doi.org/10.1080/09512748.2019.1676299>.

87. Analysts have noted that there are calls within China to adopt a launch-on-warning strategy and that it is developing the technology to enable this capability. See Acton, *Entanglement*, 79.

88. James M. Acton, *Silver Bullet? Asking the Right Questions about Conventional Prompt Global Strike* (Washington, DC: Carnegie Endowment for International Peace, 2013), xiv, <https://carnegieendowment.org/>.

89. Assessing the precise status of US-enabling capabilities is challenging because they are so highly classified. Acton, 88–90.

90. Because ICBMs and SLBMs depend on automation to set their flight trajectory and navigate to their target, they already operate de facto autonomously once launched. Thus, while autonomy enhances the strategic value of missile delivery systems, it is not an operational prerequisite—except perhaps in the underwater domain where munitions cannot be easily operated remotely.

91. Existing navigation systems tend to rely heavily on pre-mapping for navigating autonomously and identifying paths and obstacles; however, navigation systems will need to incorporate advanced vision-based guidance and built-in pre-mapping systems. Advances in machine learning techniques could significantly improve the vision-based guidance systems of these subsystems and, in turn, enable autonomy. Acton, *Silver Bullet?*, 114.

92. For example, the DOD Defense Innovation Unit plans to partner with the Joint Artificial Intelligence Center to mine large data sets across multiple aircraft platforms and ground vehicles to develop analytics and predictive maintenance applications for the US Air Force and Army.



93. So-called fire-and-forget (or semiautonomous) missiles allow the onboard sensors and computer to guide a missile to its target without further operator communications following initial target selection and fire authorization.

94. Chinese analysts have begun research into the use of big data and deep-learning AI techniques to enhance the processing speed and intelligence analysis of satellite images in support of the military's early warning capabilities, enabling a "prediction revolution" in future warfare.

95. Boulanin, *Impact of Artificial Intelligence*, 56.

96. US government-funded Sandia National Laboratories, which has made and tested hypersonic vehicles for more than 30 years, recently established an academic research coalition, Autonomy New Mexico, whose mission is to create artificially intelligent aerospace systems. Bioengineer, "Future Hypersonics Could Be Artificially Intelligent," Bioengineer.org, 18 April 2019, <https://bioengineer.org/>.

97. Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 37–73, DOI: 10.1080/01402390.2014.958150.

98. Researchers from China's People's Liberation Army (PLA) force, the College of Mechatronic Engineering and Automation of the National University of Defense Technology, Harbin University, and the Beijing Institute of Tracking and Telecommunications Technology have collaborated to address the technical challenges faced in control dynamics with HGVs.

99. These include, for example, drone swarms, robotics, precision guidance munitions, early warning systems, and cyber and electronic warfare capabilities.

100. While it is technically feasible, the United States does not currently see any role for unmanned bombers in nuclear weapons delivery.

101. Office of the Secretary of Defense, *Missile Defense Review* (Washington, DC: Department of Defense, 2019), <https://media.defense.gov/>.

102. Samuel Osborne, "Future War with Russia or China Would Be 'Extremely Lethal and Fast,' US Generals Warn," *Independent*, 6 October 2016, <https://www.independent.co.uk/>.

103. Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), 19.

# Three-Way Power Dynamics in the Arctic

REBECCA PINCUS

## Abstract

The Arctic is an emerging region of great significance to US-China-Russia great power competition. This is due to the concentration of natural resources in the Arctic, as well as its future use as a transportation corridor between the Pacific and Atlantic. Russia's dominant position in the Arctic complicates the US-China dyad. While most high-level US security strategies and discourse identify the return of great power competition as the dominant current security paradigm, China and Russia are generally treated in isolation from each other. However, when it comes to the Arctic, China-Russia cooperation is a crucial factor to consider when formulating US strategy. This article places Chinese ambitions in the Arctic in the context of Chinese grand strategy and assesses the basis of, and prospects for, Chinese-Russian Arctic cooperation. It also advances a three-track framework for understanding Chinese-Russian cooperation in the Arctic—economic, military, and political—in which issues of control and trust are contested.

\*\*\*\*\*

The Arctic is an important locus for great power competition and triangular balancing between the US, China, and Russia. It is what political science professor Rob Huebert has dubbed the “New Arctic Strategic Triangle Environment” in which “the primary security requirements of the three most powerful states are now overlapping in the Arctic region,” raising tension.<sup>1</sup> The Arctic is an emerging area of global economic activity and a highly militarized and strategic region. The future of Arctic development therefore will impact US grand strategic goals, including the international rule of law, freedom of the seas, the safety of the US homeland, and the future of NATO. Two US competitors, Russia and China, appear to have overlapping—although not well-aligned—interests in the region. The emergence of a strategic triangle complicates US and allied efforts to apply pressure to Russia in the high north, along with US efforts to counter growing Chinese global influence.

The US National Security Strategy (NSS) and National Defense Strategy (NDS) clearly identify great power competition as the dominant current global paradigm with Russia and China as US competitors. These strategies do not address the Arctic region, focusing instead on more traditional and higher-priority areas of concern. Arctic-specific discourse centers on challenges to the US posed by Russia and China. However, across both general and Arctic-specific statements of US strategy, the potential for Russia and China to cooperate in opposing US interests is largely discounted. In the Arctic, Russia and China have fundamental security interests. Thus, in the triangular geopolitical context of the region, US strategy must address the potential for China-Russia cooperation to avoid adverse policy choices.

In the 2017 National Security Strategy, the Trump administration laid out a vision for US security that warned of a new threat paradigm from states that are “steadily” implementing “long-term plans to challenge America and to advance agendas opposed to the United States, our allies, and our partners.”<sup>2</sup> The *Summary of the 2018 National Defense Strategy of the United States of America* elaborates on this vision of US security: “The central challenge to US prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers” (emphasis in original). It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations’ economic, diplomatic, and security decisions.<sup>3</sup>

The two documents are signposts for a shift in US grand strategy. They lay out holistic threats to US security and prosperity and to the global order founded on liberal democratic values. Along with others, these documents specifically identify China and Russia as peer or near-peer challengers to the US and characterize them as seeking to revise the global order: “China and Russia are now undermining the international order . . . undercutting its principles.”<sup>4</sup> The collective emphasis, here and in other foundational documents, is on the return of great power or long-term strategic competition. While US grand strategy appears to focus on the two, the NSS and NDS documents establishing this emphasis do not address the Arctic region. The Arctic has the potential to become a significant area of Sino-Russian cooperation, yet higher-level US strategy does not appear to incorporate this prospect. The core strategy documents clearly identify Russia and China as threats to US and allied interests in the Arctic but generally treat them separately.<sup>5</sup> The National Security

Strategy hints at why: “China and Russia aspire to project power worldwide, but they interact most with their neighbors.”<sup>6</sup>

Recent commentaries illustrate this interpretation. In May 2019, US secretary of state Mike Pompeo delivered the speech “Looking North: Sharpening America’s Arctic Focus” in advance of an Arctic Council ministerial meeting. In it, he sharply addresses both Chinese and Russian actions in the Arctic:

China’s words and actions raise doubts about its intentions. . . .

. . . China’s pattern of aggressive behavior elsewhere . . . should inform what we do and how it might treat the Arctic.

Let’s just ask ourselves: Do we want Arctic nations . . . ensnared by debt and corruption? Do we want crucial Arctic infrastructure to end up like Chinese-constructed roads in Ethiopia, crumbling and dangerous . . . ? Do we want the Arctic Ocean to transform into a new South China Sea? . . .

Then there’s Russia.<sup>7</sup>

Secretary Pompeo directs stern language against both Russia and China, but his remarks largely avoid the potential of meaningful cooperation between the two.

Similarly, Adm James Foggo, commander of US Naval Forces Europe–Africa and commander of NATO’s Allied Joint Force Command Naples, highlights the threats posed by Russian and Chinese actions in the Arctic. His interpretation of Sino-Russia cooperation is dismissive: “Russia and China remain wary partners, with differing stances on proposed Arctic governance and development.”<sup>8</sup> In contrast, the 2019 Chinese Defense White Paper extols Sino-Russian military cooperation:

The military relationship between China and Russia continues to develop at a high level, enriching the China-Russia comprehensive strategic partnership of coordination for a new era and playing a significant role in maintaining global strategic stability. The Chinese and Russian militaries have continued the sound development of exchange mechanisms at all levels, expanded cooperation in high-level exchanges, military training, equipment, technology and counter-terrorism, and realized positive interaction and coordination on international and multilateral occasions. Since 2012, Chinese and Russian militaries have held 7 rounds of strategic consultations. From August to September 2018, at the invitation of the Russian side, the PLA participated in Russia’s *Vostok* strategic exercise for the first time.<sup>9</sup>

Recent indications suggest that the US security establishment is finally beginning to consider Sino-Russian cooperation and pay more attention

to the Arctic region. For example, in January 2019, the director of national intelligence provided testimony specifically addressing the issue: “We anticipate that [China and Russia] will collaborate to counter US objectives. . . . The two countries have significantly expanded their cooperation, especially in the energy, military and technology spheres, since 2014.”<sup>10</sup> Recently, a series of documents explicitly connect great power competition with China and Russia to the Arctic region. The June 2019 DOD Arctic Strategy builds on the concept of great power competition outlined in the NSS and NDS. The Arctic Strategy addresses China and Russia as major concerns: “China and Russia pose discrete and different challenges in their respective theaters. . . . In different ways, Russia and China are challenging the rules-based order in the Arctic.”<sup>11</sup> Also in 2019, the US Coast Guard issued an Arctic Strategic Outlook echoing the DOD’s emphasis on great power competition in the Arctic.<sup>12</sup>

This article explores the extent of Chinese-Russian cooperation in the Arctic in three dimensions: economic, military, and political. They offer a framework for understanding Russian and Chinese interests and activities in the Arctic and for assessing what kinds of challenges may emerge for the United States. While the term “great power competition” is helpful in characterizing the overall geopolitical paradigm, it does not provide the granularity needed for defining and responding to broad challenges—like Russian and Chinese interest in Arctic development—that cut across these dimensions.

### **Economic Dimension of Sino-Russian Cooperation**

Aligning with the overall thrust of Chinese grand strategy, Beijing’s primary strategic interest in the Arctic is economic—natural resources and potential shipping lanes. Chinese-Russian cooperation centers around these two axes, both of which also align with Russian economic interests in developing its Arctic resources. In seeking to develop these resources, Russia needs foreign capital. Following the imposition of Western sanctions in 2014, Moscow clearly pivoted East and began to court Chinese investment—to the point of inviting the Belt and Road Initiative (BRI) to include Russia’s Northern Sea Route (NSR). However, Russian-Chinese economic partnership in the Arctic has foundered over issues of control.

Under the broad umbrella of economic cooperation fall two linked objectives. First is the development of the Northern Sea Route, the great shipping lane across Russia’s northern coast that connects northeast Asian ports to northern ports in Europe and North America. Second is the extraction of renewable and nonrenewable resources from the Rus-

sian Arctic Zone. (Although China is ultimately interested in trans-Arctic shipping, its ships will rely on Russian ports for refueling, resupplying, and emergency stops.)

China experts concur that economics are at the center of Chinese grand strategy. A CSIS net assessment report concludes as much, stating that “China’s economic progress, and regional economic outreach, will often be more of the central focus of its grand strategy than the modernization and expansion of its military forces.”<sup>13</sup> This interpretation is supported by Chinese documents as well. For example, China’s 2015 Military Strategy states, “Subsistence and development security concerns, as well as traditional and non-traditional security threats are interwoven. Therefore, China has an arduous task to safeguard its national unification, territorial integrity and development interests.” The strategy goes on to note that “with the growth of China’s national interests, its national security is more vulnerable to international and regional turmoil, . . . and the security of overseas interests concerning energy and resources [and] strategic sea lines of communication (SLOCs) . . . has become an imminent issue.”<sup>14</sup>

Rather than promoting a values-based agenda, Beijing appears to be positioning itself as a good partner for mutually beneficial investment and global prosperity, particularly in less-developed regions—including the Arctic. China does not appear to be intent on spreading communism, although Andrew Erickson, professor of strategy at the US Naval War College’s China Maritime Studies Institute, draws attention to some statements that indicate otherwise.<sup>15</sup> Instead, it has pursued a global agenda of win-win development in which Chinese investment, and infrastructure development in particular, provides shared prosperity. China appears to be pursuing a grand strategy based on economics rather than on values. Military strength appears to follow, rather than lead, investment. Such a development-focused path also enables China to highlight its past as a victim of imperialism and build common identity with other postcolonial states. As its 2019 Defense White Paper explains, “China has grown from a poor and weak country to be the world’s second largest economy neither by receiving handouts from others nor by engaging in military expansion or colonial plunder. . . . China has made every effort to create favorable conditions for its development through maintaining world peace, and has equally endeavored to promote world peace through its own development.”<sup>16</sup> In this way, official Chinese language connects peace and development and emphasizes identity differences between China and Western nations.

It would be sensible for an economics-based grand strategy to spread globally along trade routes and toward resource-rich areas. Indeed, this is apparent from the global pattern of Chinese investment. President Xi's emphasis on the BRI as a keystone of his foreign policy is an indication of Chinese grand strategy. The crown jewel in China's grand strategy is the BRI. A massive system of transportation and infrastructure corridors linking China with adjacent regions, the BRI promises to grow trade through increasing interconnectivity and market access. Erickson argues that Xi's signature BRI is an integral element of operationalizing current Chinese grand strategy: "[The] BRI leverages infrastructure and trade to integrate Eurasia and its periphery, perhaps ultimately within a Sinocentric geo-economic and geopolitical order."<sup>17</sup> Beyond spurring growth in target countries, the BRI will improve the flow of raw materials to China and provide new markets for Chinese goods. Of course, linking the world to China through the BRI will increase Chinese influence and position it as the go-to partner. As observes Ashley Tellis, a senior fellow at the Carnegie Endowment for International Peace, if the BRI is successful, "it will have secured political influence by serving as a new source of infrastructure investment around the world, while also acquiring new facilities for military operations along the way."<sup>18</sup>

The BRI frames China's approach to the world, including the Arctic region. China is naturally drawn to the Arctic for many reasons, such as natural resources, trade corridors (and supply route diversity), and climate change. China's grand strategy is economics-based and therefore naturally follows along global trade routes and toward natural resources. Therefore, it is not at all surprising that China should express distinct interest in the Arctic region since the Arctic basin is resource-rich. Elizabeth Wishnick, associate professor of political science at Montclair State University, points to a report from a Chinese institute affiliated with the PLA that described the Arctic "as a potential 'lifeline' for the growing Chinese economy."<sup>19</sup> As the sea ice retreats, shipping routes across the Arctic are increasingly feasible, offering desirable alternatives to current routes between China, northern Europe, and North America. While Arctic coastal states are generally high-income countries, the region as a whole suffers from a significant lack of infrastructure, further aligning the Arctic well within Chinese grand strategic parameters.

In early 2018, it was announced that Russia's Northern Sea Route would be folded into China's massive Belt and Road Initiative. Sometimes called the Arctic Silk Road or Ice Silk Road, this new crossover project has received widespread attention. According to an analysis by Yun Sun of the

Stimson Center, contrary to widespread opinion, the Russians originally proposed the Polar Silk Road.<sup>20</sup> Sun traces Russian proposals regarding the Polar Silk Road to 2015, with a follow-up proposal made by President Putin himself in 2017. Sun notes, “The pre-2014 cold-shoulder by Russia forms a sharp contrast to its enthusiasm to cooperate with China on the Northern Sea Route after the Ukraine Crisis.”<sup>21</sup> In addition, scholars Olga Alexeevna and Frederic Lasserre state that China’s BRI was perceived as a threat to Russian interests and influence in Central Asia previous to 2014, and “so the decision to officially link the Russian Arctic” to the BRI “marks an important change” and the recognition by Moscow of “the necessity to deepen Sino-Russian cooperation in the Arctic.”<sup>22</sup>

In June 2018, the China Development Bank and Russia’s Vnesheconombank (VEB) signed a deal intended to facilitate investment in Belt and Road initiatives and tie together the BRI with the Russia-led Eurasian Economic Union. The Northern Sea Route received special emphasis in the announcement of the banking agreement: while the partnership covers about 70 projects, the NSR was the only project discussed in the press release.<sup>23</sup>

Understanding the Belt and Road Initiative also benefits from an extended consideration of shipping and maritime activity in the northwestern Pacific area. An interesting aspect of Sino-Russian cooperation is the potential development of origination points for shipping from Asia. The North Korean port of Rajin has been identified as possibly a strategically critical port for China.<sup>24</sup> Other alternatives include the Russian port of Zarubino, in the process of being upgraded through combined Chinese-Russian investment. Less than a dozen miles from Chinese territory, Zarubino is less politically fraught than Rajin and also offers year-round access to the northern Pacific.<sup>25</sup> The future trajectory of Sino-Russian cooperation in the economic and military domains may intersect here.

Despite these cooperative adventures, expert opinion varies on the extent of Sino-Russian partnership regarding the NSR and the integration of the NSR into the BRI. Yun Sun, co-director of the Stimson Center East Asia Program, contends that Sino-Russian cooperation on the NSR has been held back by “divergent interests, conflicting calculations and vastly different cost-benefit analyses.”<sup>26</sup> At the same time that Chinese observers point to Russian recalcitrance, Russian commentary often pushes back. For example, Alexander Vorotnikov states that while there is shared interest in Arctic development and cooperation, “Russia takes a firm position here” (твёрдую позицию) and that “priority must remain with Russia, since the Arctic is the most important region” (Арктика



является важнейшим регионом).<sup>27</sup> The imposition of sanctions appears to have spurred Russia to more eagerly seek Chinese investment, although Russia remains a difficult partner and there are fewer tangible results than might be expected, given the level of rhetoric. One expert notes that European firms are using Chinese intermediaries to finance investments in Russia, bypassing the Western financial system altogether.<sup>28</sup>

In addition to NSR infrastructure development, Moscow and Beijing have trumpeted cooperation in the sphere of Arctic resource development, especially in oil and gas projects. In 2014, Gazprom and the China National Petroleum Corporation (CNPC) signed a contract—in the presence of Presidents Putin and Xi—obligating Gazprom to supply 38 billion cubic meters of gas annually to China for 30 years. According to Gazprom's Alexey Miller, this is “the biggest contract in the entire history of the USSR and Gazprom.”<sup>29</sup> As a resource-extractive economy, Russia depends on development of raw materials to sustain its economy. As of 2017, oil and gas exports still made up 59 percent of export goods and about 25 percent of fiscal revenue, making Russia overly reliant on these exports.<sup>30</sup> China is a resource-importing state, and therefore the marriage of Russian resources and Chinese demand might appear to be a sound basis for economic partnership.

However, like the underdevelopment of the NSR, Sino-Russian cooperation on Arctic resource projects has not yet matched the high expectations and rhetoric. A 2018 analysis by Alexeevna and Lasserre, based on Russian and Chinese data on Arctic development cooperation, reveals two interesting patterns. The first is that Sino-Russian projects in the Arctic “are frequently misrepresented” in each country and by different publications. The second is that actual projects are fewer and less successful than might be expected given the level of publicity for Sino-Russian cooperation in the Arctic. The authors note that “moving beyond political declarations is very difficult.”<sup>31</sup> They suggest that the lower-than-expected level of actual partnership is due to a mismatch of expectations: on one hand, Russians want to retain full control over Arctic development, given its strategic importance to national interests, and therefore want Chinese investment funds—without Chinese involvement in decision-making. On the other hand, Chinese investors “are reluctant to invest in very expensive and risky projects, unless they can secure a role in the management and have a voice and voting rights.” In addition, China is interested in participating in Arctic development projects to increase technological expertise and industrial capabilities, whereas Russia is generally protective of its expertise.<sup>32</sup>

Anemic development can also be partially explained by the investment climate in Russia. Analysts suggest that Russian investment protocols are neither transparent nor consistent and that regulations are frequently changed.<sup>33</sup> As one Chinese scholar observed, “the environment for investment in Russia is unfriendly. The legal system functions poorly and corruption is rampant. Russia usually pays lip service but exhibits little action in cooperation.”<sup>34</sup> Experts indicate that while Russian laws on foreign investment are very strong—“a model of clarity,” implementation is generally uneven, and “there is not much evidence regarding the effectiveness of the agencies that implement” the law.<sup>35</sup>

It appears that Russian-Chinese cooperation in the Arctic may hinge on the question of control and trust. With this in mind, the Yamal megaproject becomes especially interesting. As Alexeevna and Lasserre note, “Yamal LNG [liquefied natural gas] is a national flagship project” for Moscow, “with both economic and political implications not only for Moscow’s foreign policy but also for domestic strategy.” In a bit of uncomfortable contrast, the Yamal project is also “a showcase for China’s skills and competence in the development of Arctic resources that, in turn, will strengthen the Chinese presence in the region.”<sup>36</sup> The Yamal LNG project, which came online in 2018, made a major contribution to Russia’s economy; it increased Russian LNG production by 70.1 percent, according to Bloomberg.<sup>37</sup> Statistics reveal that “about 90% of Russia’s natural gas and about 12% of oil is today produced in the Yamal Nenets region,” and the region is anticipated to hold large additional fields, including Tambey, with more than 7 trillion cubic meters of gas.<sup>38</sup> A new giant gas project is in the works, Arctic LNG 2, located in the Gydan peninsula near the existing Yamal megaproject.<sup>39</sup> Production for the new project is estimated at nearly 20 million tons of LNG per year, most of which will be shipped via ice-capable tankers east to Asian markets.

According to expert assessments, the Russian zone of the Arctic contains potentially 48 billion barrels of oil and 43 trillion cubic meters of gas, both significant shares of total Russian reserves.<sup>40</sup> Another estimate of the overall Russian endowment is 287 billion barrels of oil equivalent.<sup>41</sup> According to data from the Organization for Economic Cooperation and Development (OECD), Russia is one of the top three oil-producing countries in the world along with Saudi Arabia and the United States.<sup>42</sup> In 2017, Russia became the largest exporter of oil in the world, surpassing both Saudi Arabia and the US.<sup>43</sup> Further, Russia is the world’s largest exporter of natural gas. The Russian companies Rosneft and Gazprom dominate the region and have exploration plans in Shtokman, near Novaya

Zemlya, as well as Yuzhno-Kirinskoye in the Far East and Leningradskoye in the Kara Sea (Gazprom). Rosneft has plans in Khatanga as well as the Barents and the Kara Seas.<sup>44</sup>

However, Beijing does not simply want to exchange cash for energy in the Arctic. China is using cooperation with Russia in the Arctic to gain expertise and know-how in the critical energy sector. Chinese firms are beginning to move into the Arctic offshore oil and gas sector, reflecting advancing technological savvy. In 2017 and 2018, a Chinese offshore oil rig, the *Nan Hai Ba Hao*, explored for oil in the Russian far north.<sup>45</sup> In 2017, the rig made a significant discovery in the Leningradskoye field, and in 2018 it explored the Rusanovskoye field, both under development by Gazprom. Guangzhou Shipyard International just completed an ice-breaking tanker with an Arc7 (highest) ice class rating, designed by Aker Arctic.<sup>46</sup> The tanker, *Boris Sokolov*, will carry LNG from Sabetta in the Yamal Peninsula to markets in Asia and Europe. It is capable of breaking up to 2 meters of ice and sailed the Northern Sea Route in January 2019 without icebreaker escort.<sup>47</sup> These signs of increasing Chinese technical capacities to operate in Arctic conditions—without dependency on Russia—may eventually change the dynamics of their relationship.

In addition to oil and gas and technical expertise in polar operations, China has a strategic interest in Russian minerals in the Arctic. Jiayu Bai of the Ocean University of China, and Alexandr Voronenko, now executive director, Research Center for Shanghai Cooperation Organization and Asia Pacific Region, also highlight potential Russian-Chinese cooperation on rare earths mining in the Arctic. These strategic minerals are important to many advanced electronics and military systems. Rare earth deposits have been identified in the Kola and Taimyr Peninsulas and in Yakutia, and talks between Nor Nickel and General Nice Group (which is also developing rare earths in Greenland) are “in progress.”<sup>48</sup> A 2017 CNA report detailed Russian mining prospects and deposits.<sup>49</sup> Mining in the Russian Arctic connects to broader strategic resource goals for Beijing, which has global interests in rare earth elements.

Another Arctic resource that may be of interest to China is seafood. The world’s two most productive fisheries are found in the region: the Barents Sea and the Bering Sea fisheries. As yet, there is no commercial fishery in the central Arctic Ocean; in fact, in 2017, a group of Arctic and non-Arctic states, including China, signed an agreement to hold off on fishing in the central Arctic.<sup>50</sup> The moratorium is intended to give scientists enough time to adequately understand the structure of Arctic fisheries and prepare sustainable fisheries management plans. Chinese influence has

been identified in the process of negotiating the moratorium.<sup>51</sup> As global fisheries decline, the as yet untapped seafood resources of the central Arctic Ocean may be increasingly in demand.<sup>52</sup>

While their interests align (Russia as a resource vendor, China as a resource client), their cooperation has been impeded by each partner's desire to maintain control or a leading position in projects. Russian interests in partnering with China were clearly given a boost following the 2014 sanctions. The stakes for US strategy are clear: in a triangular context, US efforts to weaken Russia's economy may strengthen China's economic influence in Moscow and its political cooperation.

### Political Dimension

China is building relationships with all the Arctic states to increase its influence over decisions about the future of the Arctic region. The political dimension offers a relatively direct collision between Chinese and Russian long-term grand strategic objectives. Russia has traditionally been jealously protective of its special position in the Arctic region. In contrast, Beijing is seeking to legitimate its interest in the region and gain a shaping role in the future of Arctic development. Partnering with Russia, the dominant Arctic power, is unmistakably desirable although complicated.

In this, Russia is made less vulnerable by its status as the Arctic superpower; however, the underdeveloped and brittle Russian economy acts as a constraint on Moscow's freedom of action. Chinese-Russian cooperation was given a jolt in 2014 when Western countries imposed sanctions on Russia in response to its annexation of Crimea. Suddenly cut off from access to Western capital and partnering for Arctic energy projects, Russia pivoted East.

In the short term, Arctic cooperation suits both Chinese and Russian strategic interests and complicates US objectives. From a geographic perspective, Russia dominates the Arctic basin. The prospect of effective Sino-Russian cooperation therefore raises the possibility of a localized sphere in which the capacity of the PRC could operate in conjunction with Russian geography to create an Arctic trajectory outside the system of international rule of law.

The Chinese journal *Advances in Polar Science* published an article co-authored by Russian and Chinese scholars directly addressing Sino-Russian cooperation in the Arctic region. The authors summed up the alignment of Russian and Chinese interests in the Arctic: "Russia is interested in Chinese investments and technology; in turn, Russia can grant China access to mineral resources and the NSR. . . . Furthermore, through

cooperation with Russia, China can expand its role in the Arctic [C]ouncil and the process of formulating the regional agenda.” The authors observed that Russia and China “can play a major role in forming the system of international relations in the Arctic using their advantages and authority.” In addition, “cooperation with Russia will give Chinese actions in the region more validity.”<sup>53</sup>

Beijing is clearly aware that its efforts to gain a seat at the Arctic table have not been uniformly welcomed and that Russia in particular has mixed opinions. The executive director for the Institute for China-America Studies, Nong Hong, observes that “unfortunately, China’s intentions have been met with suspicion by Arctic states” and identifies Russia, Canada, and Iceland as the most “vigilant”; she specifically cites “the vigilance of the Russian military” regarding Chinese interest in the Arctic.<sup>54</sup>

One means of gaining entrée into Arctic governance is through participation in the Arctic Council: China was granted observer status at that forum in 2013 after some years of effort. In part, the delay in admitting China to the Arctic Council as an observer was due to Russian reluctance: “the Russian government initially expressed wariness about allowing Beijing any formal role within the organization,” according to Marc Lanteigne (Massey University, Auckland).<sup>55</sup> However, other observers also point to Canadian reluctance to admit China and other observers.<sup>56</sup> Established in 1996, the Arctic Council is the highest-level intergovernmental forum and *de facto* governance organization for the region. While only the eight Arctic states have votes at the Arctic Council, the indigenous peoples of the Arctic region are represented by their organizations as Permanent Participants and can fully participate in discussions. In addition to these participatory categories, there is a category of Observer states and organizations. Observers do not have equal right to participate in council discussions but may attend meetings and participate on invitation.

In January 2018, the State Council Information Office of China published the white paper “China’s Arctic Policy.” This long-anticipated statement of China’s official Arctic policy has received a great deal of analysis. A helpful explanation came in March 2018 from the Washington-based, Chinese-funded Institute for China-America Studies. This report clearly states China’s approach to gaining influence in Arctic decision-making:

China is also active in promoting bilateral relations with Arctic states for strategic purposes. . . . China should deal with Arctic states on an individual basis. . . . This way, China will have much more leeway for strategic operations. This one-on-one model is similar to China’s stance in the

South China Sea issue, where China insists on bilateral rather than multilateral negotiation. . . .

China is also focusing on improving diplomatic relations with the five North European nations: Iceland, Denmark, Norway, Sweden and Finland. Cooperation with these countries is not only aimed at acquiring resources, but also to expand[ing] China's influence in the Arctic. . . . The Northern European states are not strong enough to compete with Russia or with their ally the United States—both state parties in the Arctic region—so these states are willing to turn to China for help. If China can establish a long-term strategic cooperation mechanism on Arctic affairs with the Northern European states, it will achieve a greater say in Arctic affairs.<sup>57</sup>

As this quote illustrates, Russia is not the only focus of Chinese interest in the Arctic. In fact, China's influence-seeking strategy may be even more of a problem for the United States vis-a-vis the small Nordic countries, which may be more vulnerable.

The example of Norwegian-Chinese relations is illustrative. In 2010, following the awarding of the Nobel Peace Prize to Chinese dissident Liu Xiaobo "for his long and non-violent struggle for fundamental human rights in China," the Chinese government retaliated by imposing import controls on Norwegian salmon that effectively closed the market.<sup>58</sup> For six years, Norway worked to restore relations with Beijing, finally succeeding in 2016—at the cost of an extraordinary joint declaration:<sup>59</sup>

Due to the Nobel Peace Prize award and events connected to the Prize, China-Norway relations have deteriorated. The Norwegian side is fully conscious of the position and concerns of the Chinese side and has worked actively to bring the bilateral relations back to the right track. . . .

The Norwegian Government reiterates its commitment to the one-China policy, fully respects China's sovereignty and territorial integrity, attaches high importance to China's core interests and major concerns, will not support actions that undermine them, and will do its best to avoid any future damage to the bilateral relations.<sup>60</sup>

As the Norwegian example demonstrates, Beijing is willing to use its advantageous trade position relative to smaller states—even formidable small states like Norway—to extract significant political concessions and deference. Therefore, economic leverage may pave the way for political goals to be achieved. The hallmark of grand strategy is the leveraging of all means of state power toward overarching objectives, and Norway's experience provides a clear example of Beijing's capabilities. This instance also gives a clear warning to Russia about the possible consequences of over-

reliance on China for capital and markets. Moscow has been making clear efforts to diversify its sources of investment into Arctic oil and gas projects, possibly to backstop against this danger.

Chinese-Russian cooperation in the Arctic can be understood as an unresolved balancing act between the two states. Russia needs outside capital to fund Arctic development but seeks to maintain control—both politically and over specific investment projects. China wants access to both Arctic resources and the political decision-making process and is willing to use economic tools as leverage. A third dimension is important to understanding the prospects for Russian-Chinese cooperation in the Arctic: military security. While this is the least-developed area of cooperation, it also has the potential to pose the most direct threat to the United States.

### **Military Dimension**

Many signs point to a growing security partnership between China and Russia. In October 2019, President Putin stated that Russia is “helping our Chinese partners” develop an antimissile early warning system.<sup>61</sup> He also described Russian-Chinese relations as “an allied relationship in the full sense of a multifaceted strategic partnership.”<sup>62</sup> While China has no Arctic military presence, it maintains interests in the region as stated above. Therefore, assessing the current level of, and prospects for, Chinese-Russian security cooperation is crucial to understanding the overall prospects for great power competition in the Arctic.

The Arctic is a security bastion for Russia, and therefore this dimension of potential Russia-China cooperation is of great sensitivity. The Russian navy and some other elements of the Russian military have been hawkish on China, and in some parts of Russia—particularly the Far East—Chinese influence is perceived as a potential threat. China appears to be seeking polar capabilities, including icebreakers and polar-capable submarines. The two countries have been ramping up joint military exercises and operations recently, including in near-Arctic areas. The future of Sino-Russian military cooperation in the Arctic will directly affect the security position of the US and its NATO allies in the region. As in the economic dimension, while security cooperation serves Chinese and Russian interests in balancing against the US, there is deep-rooted friction that may ultimately sink cooperation.

Some observers note the strategic military interest China may have in the Arctic. The Fort Greely missile complex could potentially be directed against China, and northern deep-water routes might offer desirable sub-

marine routes.<sup>63</sup> Arctic routes also offer China an alternative to the Malacca dilemma and would bolster its security by having Russian oil as a strategic alternative to the Middle East. Yang Zhirong of the People's Liberation Army Navy (PLAN) Naval War College states that China should develop a military component to its Arctic strategy. It would include "dedicating naval staff to Arctic affairs, as well as information-gathering, developing Arctic-capable equipment, improving communication in the region, making ports of call visits," and recognizing the strategic importance of the Arctic.<sup>64</sup> The journey of PLAN vessels to the Baltic Sea, including port calls in Finland and exercises with Russian navy ships in 2017, can be interpreted through this lens.

Sino-Russian military cooperation outside the Arctic region has grown in recent years and received widespread attention. Relevant PRC-Russia military cooperation includes arms sales and a growing number of live exercises. According to a recent DOD report, in September 2017 the Chinese and Russian navies conducted exercises—including antisubmarine, submarine rescue, and joint air defense—in the Baltic Sea and Sea of Okhotsk, both adjacent to the Arctic region.<sup>65</sup> These were the sixth joint exercises since 2012. The Sea of Okhotsk is interesting in that it is also a "Russian lake" that is key to Russian Arctic and Asian strategy, as Stephen Blank of the American Foreign Policy Council has argued, and therefore Russian-Chinese joint exercises there are suggestive of a closer functioning relationship.<sup>66</sup>

PLAN submarine operations already include the North Atlantic, and observers maintain that Arctic operations are likely to soon become an element of PLAN missions.<sup>67</sup> One of the joint Sino-Russian military design and construction programs underway is focused on diesel-electric submarines.<sup>68</sup> While a Chinese submarine has not yet surfaced in the Arctic Ocean, that achievement is considered likely within a decade, according to Lyle Goldstein of the China Maritime Studies Institute.<sup>69</sup> In support of this belief, he points to an April 2018 paper in a leading Chinese scientific journal, the *Chinese Journal of Ship Research*, on submarine hull design for surfacing through ice. The abstract for this paper notes, "With deepening research on the geographical and climatic environment of the Arctic, the political and military value of submarines in the region has been well recognized."<sup>70</sup>

The Chinese navy is increasingly focused on long-range missions that will take its platforms farther and for longer periods. By 2020, according to a 2018 OSD assessment, China will likely field between 69–78 submarines, mostly diesel attack but with some SSBNs and SSNs.<sup>71</sup> By the early



2020s, China will begin construction on its next-generation SSBNs, the Type 096, to be armed with JL-3 SLBMs. A 2015 Office of Naval Intelligence report, while not mentioning the Arctic specifically, comments that the PLAN is increasingly “expected to defend major SLOCs” and that this new and expanding role for the Chinese Navy will demand “the capability to sustain a maritime presence in strategic locations, in hostile conditions, and for extended periods.”<sup>72</sup> China and the PLAN are moving purposefully in the direction of multimission naval capabilities in service of grand strategic objectives “to preserve China’s interests and commensurate with its role as an emerging major power.” In addition, Chinese ocean science in support of military operations and seabed mining is highly advanced and may surpass US efforts.<sup>73</sup> China’s military spending has increased in recent years in line with its economic growth. President Xi has made public declarations of his intent to modernize the Chinese military into a multi-theater force.<sup>74</sup>

China has recently embarked on an icebreaker building program: its first icebreaker, the *Xue Long*, was purchased; it recently completed domestic construction of its second, the *Xue Long 2*; and in June 2018, the Chinese nuclear corporation opened a call for bids for the country’s first nuclear-powered icebreaker.<sup>75</sup> While China has two icebreakers already, a nuclear-powered icebreaker would mark both a significant advance in polar capabilities and a step toward fielding a nuclear-powered carrier. The construction of the nuclear-powered icebreaker appears to be part of a broader Chinese effort to develop domestic nuclear propulsion and reactor technology expertise.<sup>76</sup>

The military cooperation between China and Russia has been described as “a more balanced (though limited) security partnership between two countries that are neither adversaries nor allies, but share certain security concerns such as . . . balancing the United States and its allies.”<sup>77</sup> The extent to which Russia is willing to share its expertise in Arctic submarine operations with China may indicate the limits of their security partnership. Cooperation on joint submarine production and joint exercises on submarine rescue suggest that Russia is sharing expertise with the PLAN.

Any Sino-Russian security partnership in the Arctic will be vastly complicated by the high priority of the Arctic in Russia’s overall grand strategy. The Arctic region is a core national interest for Russia. A NATO analysis of Russian Arctic strategy and policy concluded in 2018 that Russian policy language reflects an increased emphasis on national security in the Arctic and a growing belief that “security is a precondition for successful resource development” in the Russian Arctic.<sup>78</sup> In recent years, Moscow

has made strong statements of its intentions to build out the military infrastructure required to fully secure the Russian Arctic. While these declarations of intent have not yet been fully funded, some construction has indeed moved ahead.<sup>79</sup>

Of note, in December 2014 Russia established the Arctic Joint Strategic Command (AJSC). In addition, Russia has moved ahead with upgrading and extending its airfields along its northern perimeter. To the west, on Franz Josef Land, the Nagurskoye air base was shown off in 2017 with great fanfare.<sup>80</sup> The base has a 2,500-meter airfield that was recently resurfaced to accommodate heavy planes year-round.<sup>81</sup> In December 2015, the AJSC received its own air force and army with the formation of the 45th Air Force and Air Defense Army of the Northern Fleet. According to Russian sources, 50 bases are expected to be built across the Arctic.<sup>82</sup> Russia is reportedly developing polar-adapted versions of the Pantsir surface-to-air missile and the S-400 anti-aircraft system.<sup>83</sup> The AJSC controls all of these resources, in addition to other combat units, radar stations, and other units in the region. As one expert remarks, “Rebuilding and upgrading regional military infrastructure and enhancing command and control have emerged as consistent themes in Russia’s strategic thinking on the Arctic. [Creating] the [AJSC] as the fifth military district of Russia, with the Northern Fleet as its mainstay, reflected the priority that Russia began to attach to the defense of the Arctic.”<sup>84</sup>

It is important to underline that the Arctic is a core national interest for Russia. If Russia’s leaders indeed have a grand strategy, developing the Arctic is one of its objectives. In addition, the bulk of Russia’s strategic forces are concentrated in the Kola Peninsula in the western Arctic. As a result, the Arctic is among the most sensitive parts of Russia and among its top security priorities.

Chinese experts appear to recognize that Russia perceives a security problem in the Arctic. One of China’s leading scholars of international politics wrote, “Russia’s northern border is no longer peaceful. As for China, developing strategic ties with Russia can help it in ‘stabilizing its northern border so that it can turn to the ocean’—in other words it can give it more space to deal with maritime disputes with its southern neighbors.”<sup>85</sup> In the context of a strategic triangle in the Arctic, China benefits from a Russian security focus on the US and NATO.

Deepening Chinese and Russian military cooperation may be in response to increasing tension with the United States. While China does not yet have a military presence in the Arctic, it appears to be pursuing both icebreaker and Arctic submarine capabilities. China’s interest in ac-

cessing and protecting strategic Arctic SLOCs, which provide it access to strategic resources and an alternative to Malacca, makes sense in a Russia partnership context. In seeking to secure its Arctic resources and territory, Russia may welcome Chinese arms purchases and the counterbalance a Chinese partnership provides against the US. However, a great deal of tension is inherent in this developing partnership. As China becomes increasingly Arctic-capable, how will Beijing and Moscow manage their relationship? How can the US best manage competition without providing more impetus for Chinese-Russian alignment?

## **Conclusion**

Many analysts point to 2014 as a turning point in Russia-China relations overall and in Arctic cooperation more specifically.<sup>86</sup> Frankly, many observers identify a downturn in US/West–Russia relations—particularly the sanctions—as pushing Russia toward China.<sup>87</sup> Multiple scholars, including Evan Medeiros and Michael Chase, have observed that “for China, the Western sanctions on Russia . . . were a welcome buying opportunity.” China was happy to fill the market gap created by sanctions.<sup>88</sup> Liu Fenghua of the Chinese Academy of Social Sciences remarked in 2016 that “since the outbreak of the Ukraine crisis, the US has once again chosen to contain China and Russia simultaneously, thus greatly enhancing a China–Russia strategic partnership.”<sup>89</sup> While the sanctions are an important element of the broader US–Russia relationship, their effect on Sino-Russian cooperation in the Arctic may be an unintended outcome.

While US discourse frequently lumps China and Russia together, it generally does not follow through to consider the implications or effects of this pairing. There is not yet clear evidence that US strategists are taking seriously the prospect of cooperation between China and Russia in the Arctic region. By symbolically grouping China and Russia together as competitors, the US may inadvertently provide impetus for more substantive Sino-Russian cooperation. Given Russia’s influence and dominant geographic position in the Arctic region, this consequence may be costly.

This article has argued for the importance of the Arctic to China at a grand strategic level, including economic, political, and military elements. Russia’s dominant position in the Arctic region and avowed interest in challenging American global leadership make Russia a natural partner of interest for China. Sino-Russian cooperation in the Arctic serves the short-term interests of both states as well as longer-term Chinese goals. However, Russia does not want to be a junior partner to China. Moreover, Russia’s strategic military position in the Arctic region would be chal-

lenged by a Chinese military presence there, and therefore significant questions remain about the long-term viability of Sino-Russian partnership as China moves further toward its goal of fielding a multi-theater modern military force.

The central position of Russia in the Arctic lays bare the discontinuities in US strategy: at least in the Arctic, it is problematic to treat China and Russia as separate strategic rivals. Their emerging partnership in the region is fitful and laced with fissures, but current US policies of applying pressure drive them closer together—as the aftereffects of the sanctions regime demonstrate. In the context of a strategic triangle in the Arctic, US strategy toward either China or Russia must be considered in tandem. Actions taken toward one will invariably affect the other given the close linkages in the region.

In July 2019, the first-ever China-Russia joint air patrol made headlines around the world when one of the Russian A-50s violated South Korean airspace over the Dokdo/Takeshima Islands.<sup>90</sup> As one commentator concluded, “the Russo-Chinese ‘strategic partnership’ is now a force to be reckoned with. . . . Seoul and Tokyo should no longer see the US as the sole military hegemon in the region.”<sup>91</sup> The bold actions taken in concert by Russia and China may reflect growing confidence in their strategic partnership. Under pressure from the US, both China and Russia may determine that continuing to work together may be advantageous. The Arctic is a natural place for this cooperation to grow.

The future contours of Arctic development and governance are elastic. While the extent to which China and Russia will be able to meaningfully cooperate to shape the region is unclear, the US has begun to actively grapple with the concept of great power competition with both. However, it appears that US strategy has not yet fully engaged the ramifications of growing Sino-Russian cooperation across economic, military, and political dimensions in the Arctic region. Without a linked strategic approach, the US runs the risk of strategic misstep. **SSQ**

#### **Rebecca Pincus**

Dr. Pincus is an assistant professor in the Strategic and Operational Research Department at the US Naval War College and focuses on Arctic security and politics. The views and opinions presented here are her own and do not represent the official position of the Naval War College, United States Navy, or DOD. This article refines ideas first presented in her testimony before the US-China Economic and Security Review Commission on 21 March 2019 (see report at <https://www.uscc.gov/>). Dr. Pincus thanks the China Maritime Studies Institute at the Naval War College for helpful suggestions and feedback.

## Notes

1. Rob Huebert, "The New Arctic Strategic Triangle Environment (NASTE)," in *Breaking the Ice Curtain: Russia, Canada, and Arctic Security in a Changing Circumpolar World*, eds. P. Whitney Lackenbauer and Suzanne Lalonde (Calgary: Canadian Global Affairs Institute, 2019), 76, <https://www.academia.edu/>.
2. President Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, 2017), 2, <https://www.whitehouse.gov/>.
3. 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: Department of Defense, 2018), 2, <https://dod.defense.gov/>.
4. Department of Defense, *Summary of the 2018 National Defense Strategy*, 2.
5. A December 2018 DOD report focused on China, although it listed expanding military cooperation between China and Russia and noted that the Belt and Road Initiative includes the Arctic Ocean. Department of Defense, *Assessment on U.S. Defense Implications of China's Expanding Global Access* (Washington, DC: Department of Defense, December 2018), 12, <https://media.defense.gov/>.
6. Trump, *National Security Strategy*, 45.
7. Secretary Michael R. Pompeo, "Looking North: Sharpening America's Arctic Focus" (speech, Rovaniemi, Finland, 6 May 2019), <https://www.state.gov/>.
8. Adm James Foggo III, "Russia, China Offer Challenges in the Arctic," *Defense One*, 10 July 2019, <https://www.defenseone.com/>.
9. State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, Defense White Paper (Beijing: State Council Information Office, People's Republic of China, July 2019), full text posted by Andrew S. Erickson on his website, <http://www.andrewerickson.com/>.
10. Daniel R. Coats, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 29 January 2019), 24, <https://www.odni.gov>.
11. Office of the Under Secretary of Defense for Policy, *Report to Congress: Department of Defense Arctic Strategy* (Washington, DC: Department of Defense, June 2019), 6, <https://media.defense.gov/>.
12. United States Coast Guard, *Arctic Strategic Outlook: The United States Coast Guard's Vision for the Arctic Region* (Washington, DC: US Coast Guard, April 2019), <https://www.uscg.mil/>.
13. Anthony H. Cordesman, with Max Molot, "China and the U.S.: Cooperation, Competition and/or Conflict: An Experimental Assessment," working draft (Washington, DC: Center for Strategic and International Studies, 1 October 2019), <https://www.csis.org/>.
14. The State Council Information Office of the People's Republic of China, *China's Military Strategy 2015*, white paper (Beijing: State Council Information Office of the People's Republic of China, 2015), Jamestown Foundation, China Brief, 4–6, <https://jamestown.org/>.
15. He quotes Xi, "China's success proves that socialism can prevail and be a path for other developing countries to emulate and achieve modernization." Andrew S. Erickson, "China," in *Comparative Grand Strategy: A Framework and Cases*, eds. Thierry Balzacq,

Peter Dombrowski, and Simon Reich (Oxford: Oxford University Press, 2019), 86, <http://www.andrewerickson.com/>.

16. State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 8.

17. Erickson, "China," 83–84.

18. Ashley J. Tellis, "Pursuing Global Reach: China's Not So Long March toward Preeminence," in *Strategic Asia 2019: China's Expanding Strategic Ambitions*, eds. Ashley J. Tellis, Alison Szalwinski, and Michael Wills (Seattle, WA: The National Bureau of Asian Research, 2019), 34.

19. Elizabeth Wishnick, *China's Interests and Goals in the Arctic: Implications for the United States*, The Letort Papers (Carlisle, PA: Strategic Studies Institute, US Army War College, 2017), 37.

20. Yun Sun, *The Northern Sea Route: The Myth of Sino-Russian Cooperation* (Washington, DC: Stimson Center, East Asia Program, 5 December 2018), 2–3, <https://www.stimson.org/>.

21. Sun, 7.

22. Olga Alexeevna and Frederic Lasserre, "An Analysis on Sino-Russian Cooperation in the Arctic in the BRI Era," *Advances in Polar Science* 29, no. 4 (30 December 2018): 276.

23. Atle Staalesen, "Chinese Money for Northern Sea Route," *The Barents Observer*, 12 June 2018, <https://thebarentsobserver.com/>.

24. For more on Rajin/Rason, see Salvatore Babones, "If North Korea Opens Up, Rason Could Become North Korea's Shenzhen." *Forbes*, 2 May 2018. <https://www.forbes.com/>.

25. For more on Zarabino, see Michael Lipin, "China's Landlocked Northeast Turns to Russian Port as Trade Outlet," *Voice of America (VOA) News*, 28 September 2014, <https://www.voanews.com/>.

26. Yun Sun, *The Northern Sea Route: The Myth of Sino-Russian Cooperation* (Washington, DC: Stimson Center, East Asia Program, 5 December 2018), <https://www.stimson.org/>.

27. Aleksander Vorotnikov, "Чем выгодно России сотрудничество с Китаем по Арктике? [How does Russia benefit from cooperation with China in the Arctic?]", *Regions*, 9 July 2018. Thanks to Dr. Lyle Goldstein for highlighting this article. Quotation originally appeared in testimony from Dr. Rebecca Pincus in *An Emerging China-Russia Axis? Implications for the United States in an Era of Strategic Competition: Hearing before the U.S.-China Economic and Security Review Commission*, 116th Cong., 1st sess., 21 March 2019, 197, <https://www.uscc.gov/>.

28. Nikolas K. Gvosdev, "How Europe and Russia Are Fighting U.S. Sanctions," *The National Interest*, 6 October 2018, <https://nationalinterest.org/>.

29. "Alexey Miller: Russia and China Signed the Biggest Contract in the History of Gazprom," Gazprom, press release, 21 May 2014, <http://www.gazprom.com/>. The Russian company Gasprom also noted that "USD \$55 billion will be invested in construction of production and transmission facilities in Russia" (ibid.).

30. In addition, metals made up another 10.4 percent of exports; overall, raw materials (including energy products, metals, wood products, precious metals and stones, and other minerals) comprised well over three-fourths of Russia's exports. World Bank Group, *Preserving Stability; Doubling Growth; Halving Poverty—How?*, Russia Economic Report No. 40 (Washington, DC: World Bank Group, November 2018), 20.

31. Alexeevna and Lasserre, "An Analysis on Sino-Russian Cooperation," 274.

32. Alexeevna and Lasserre, 276.

33. Alexeevna and Lasserre, 271.
34. Chen Yu, "On 'Pivot to East' in Russian Diplomacy," *Contemporary International Relations* 26, no. 6 (2016): 22.
35. Mark E. Rosen and Cara B. Thuringer, *Unconstrained Foreign Direct Investment: An Emerging Challenge to Arctic Security* (Arlington, VA: Center for Naval Analyses, November 2017), 45–46.
36. Alexeevna and Lasserre, "An Analysis on Sino-Russian Cooperation," 277.
37. Leonid Bershidsky, "Russia's Growth Expectations Fall Back to Earth," Bloomberg, 13 February 2019, <https://www.bloomberg.com/>.
38. Atle Staalesen, "Under the Surface of Russia's Arctic Super-Region Is a Looming Disaster," *The Barents Observer*, 17 January 2019, <https://thebarentsobserver.com/>.
39. Atle Staalesen, "Frenchmen Sign Landmark Deal with Novatek, Boost Presence in Russian Arctic," *The Barents Observer*, 5 March 2019, <https://thebarentsobserver.com/>.
40. Stanislav Pritchin, "Russia's Untapped Arctic Potential," Chatham House, 29 January 2018, <https://www.chathamhouse.org/>.
41. Rosen and Thuringer, *Unconstrained Foreign Direct Investment*, 20.
42. OECD, Crude oil production (indicator), accessed 7 March 2019, <https://doi.org/10.1787/4747b431-en>.
43. Apurva Sanghi et al., *Russia Economic Report: Preserving Stability; Doubling Growth; Halving Poverty—How?*, Russia Economic Report no. 40 (Washington, DC: World Bank Group, November 2018), 17, <http://documents.worldbank.org/>.
44. Jason Corcoran, "Russia Seeks to Revive Offshore Arctic Ambitions," *Petroleum Economist*, 6 March 2018, <https://www.petroleum-economist.com/>.
45. The Chinese rig was brought to Russia by the Chinese heavy-lift vessel *Hai Yang Shi You* 278. Atle Staalesen, "Chinese Oilmen Ready to Go Home after 5 Months in Russian Arctic," *The Barents Observer*, 22 November 2018, <https://thebarentsobserver.com/>.
46. Atle Staalesen, "New Condensate Tanker Sails North, Gets Ready to Break Ice on Northern Sea Route," *The Barents Observer*, 6 December 2018. <https://thebarentsobserver.com/>.
47. Atle Staalesen, "Two New-Built Tankers Are Crossing the Arctic in Midwinter," *The Barents Observer*, 11 January 2019, <https://thebarentsobserver.com/>.
48. Jiayu Bai and Alexandr Voronenko, "Lessons and Prospects of Sino-Russian Arctic Cooperation," *Advances in Polar Science* 27, no. 3 (September 2016): 188, <http://www.aps-polar.org/>.
49. Rosen and Thuringer, *Unconstrained Foreign Direct Investment*, 25.
50. See NOAA Fisheries, "U.S. Signs Agreement to Prevent Unregulated Commercial Fishing on the High Seas of the Central Arctic Ocean," 3 October 2018, <https://www.fisheries.noaa.gov/>.
51. Nengye Liu, "How Has China Shaped Arctic Fisheries Governance?," *The Diplomat*, 20 June 2018, <https://thediplomat.com/>.
52. According to a study by the European Commission's Joint Research Center, China is the world's largest consumer of seafood on a total basis, at 65 million tons annually, although it is ranked only seventh in per capita seafood consumption. European Commission, "How Much Fish Do We Consume? First Global Seafood Consumption Footprint Published," EU Science Hub, 27 September 2018, <https://ec.europa.eu/>.
53. Bai and Voronenko, "Lessons and Prospects," 185–91.

54. Nong Hong, *China's Interests in the Arctic: Opportunities and Challenges; Examining the Implications of China's Arctic Policy White Paper* (Washington, DC: Institute for China-America Studies, March 2018), 17–18, <https://chinaus-icas.org/>.
55. Marc Lanteigne, "Northern Crossroads: Sino-Russian Cooperation in the Arctic," National Bureau of Asian Research, 27 March 2018, <https://www.nbr.org/>.
56. Wishnick, *China's Interests and Goals in the Arctic*, 33.
57. Hong, *China's Interests in the Arctic*.
58. The Norwegian Nobel Committee, "The Nobel Peace Prize for 2010," 8 October 2010, <https://www.nobelprize.org/>. For example, see Mark Lewis, "Norway's Salmon Rot as China Takes Revenge for Dissident's Nobel Prize," *Independent*, 6 October 2011, <https://www.independent.co.uk/>.
59. For additional coverage, see Sewell Chan, "Norway and China Restore Ties, 6 Years after Nobel Prize Dispute," *The New York Times*, 19 December 2016, <https://www.nytimes.com/>.
60. Government of Norway, Ministry of Foreign Affairs, "Full Normalisation of Relations with China," press release, 19 December 2016, with link to joint statement: Statement of the Government of the People's Republic of China and the Government of the Kingdom of Norway on Normalization of Bilateral Relations, <https://www.regjeringen.no/>.
61. Stepan Kravchenko, "Putin Says Russia Is Helping China Build Missile Warning System," *Bloomberg*, 3 October 2019, <https://www.bloomberg.com/>.
62. Vasily Kashin, "Russia and China Take Military Partnership to New Level," *Moscow Times*, 23 October 2019, <https://www.themoscowtimes.com/>.
63. Elizabeth Wishnick, *China's Interests and Goals in the Arctic*, 29.
64. Wishnick, 32.
65. Department of Defense, *Implications of China's Expanding Global Access*, 8.
66. Stephen Blank, "The Arctic and Asia in Russian Naval Strategy," *The Korean Journal of Defense Analysis* 29, no. 4 (2017): 575–97.
67. Joseph Trevithick, "The Scope, Not the Scale, of Russian and Chinese Naval Ops in the Atlantic Is Worrisome," *The Drive*, 10 August 2018, <http://www.thedrive.com/>.
68. Department of Defense, *Implications of China's Expanding Global Access*, 15.
69. For more on Sino-Russian security cooperation, see Lyle J. Goldstein, "A China-Russia Alliance?," *The National Interest*, 25 April 2017, <https://nationalinterest.org/>; Lyle J. Goldstein, "The Real Russia-China Connection That Should Worry America," *The National Interest*, 22 January 2017, <https://nationalinterest.org/>; and Lyle J. Goldstein, "Does China Need Allies?," *The National Interest*, 31 March 2016, <https://nationalinterest.org/>.
70. Ye Liyu et al., "Peridynamic Model for Submarine Surfacing through Ice," *Chinese Journal of Ship Research* 13, no. 2 (April 2018). Thanks to Lyle Goldstein for bringing this paper to light.
71. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018* (Arlington, VA: Department of Defense, 16 August 2018), 28–29, <https://media.defense.gov/>.
72. Office of Naval Intelligence, *The PLA Navy: New Capabilities and Missions for the 21st Century* (Washington, DC: Office of Naval Intelligence, 2015), 9, <https://fas.org/>.
73. Ryan D. Martinson and Peter A. Dutton, *China Maritime Report No. 3: China's Distant-Ocean Survey Activities: Implications for U.S. National Security*, CMSI China Maritime Reports (Newport, RI: China Maritime Studies Institute, US Naval War College, November 2018), 3, <https://digital-commons.usnwc.edu/>.



74. To that end, in 2019 China plans to grow its defense spending by 7.5 percent; SIPRI estimates that Beijing devotes roughly 2 percent of GDP to military spending. After the US, China is now the second-largest military spender in the world. David Tweed, "China Defense Spending Set to Rise 7.5% as Xi Builds Up Military," *Bloomberg*, 4 March 2019, <https://www.bloomberg.com/>.

75. Kyle Mizokami, "China Is Planning a Nuclear-Powered Icebreaker," *Popular Mechanics*, 25 June 2018, <https://www.popularmechanics.com/>.

76. Trym Aleksander Eiterjord, "Checking in on China's Nuclear Icebreaker," *The Diplomat*, 5 September 2019, <https://thediplomat.com>.

77. Richard Weitz, *Parsing Chinese-Russian Military Exercises*, the Letort Papers (Carlisle, PA: Strategic Studies Institute and US Army War College Press, April 2015), 2, <https://publications.armywarcollege.edu/>.

78. Nazrin Mehdiyeva, *Russia's Arctic Papers: The Evolution of Strategic Thinking on the High North*, Russian Studies Series 4/18 (Rome: NATO Defense College, 19 November 2018), <http://www.ndc.nato.int/>.

79. For a full analysis, see Mathieu Boulègue, *Russia's Military Posture in the Arctic: Managing Hard Power in a 'Low Tension' Environment* (London: Chatham House [the Royal Institute of International Affairs], June 2019), <https://www.chathamhouse.org/>.

80. For example, see Thomas Nilsen, "Take a Look Inside Russia's Northernmost Arctic Military Base," *The Barents Observer*, 18 April 2017, <https://thebarentsobserver.com/>.

81. Atle Staalesen, "Russia Giving Major Upgrade to Airstrip in High Arctic," *Eye on the Arctic*, 27 September 2018, <http://www.rcinet.ca/>.

82. See Mehdiyeva, *Russia's Arctic Papers*.

83. Mary Ilyushina and Frederik Pleitgen, "Inside the Military Base at the Heart of Putin's Arctic Ambitions," *CNN*, 5 April 2019, <https://edition.cnn.com/>.

84. Mehdiyeva, *Russia's Arctic Papers*.

85. Wang Sheng and Luo Xiao, "Building a New Type of Sino-Russian Relationship," *Contemporary International Relations* 23, no. 5 (2013): 91.

86. For example, see Alexeevna and Lasserre, "An Analysis on Sino-Russian Cooperation."

87. See Alexeevna and Lasserre.

88. Michael S. Chase et al., *Russia-China Relations: Assessing Common Ground and Strategic Fault Lines*, Special Report #66 (Seattle, WA: The National Bureau of Asian Research, 2017), 9, <https://www.nbr.org/>.

89. Liu Fenghua, "China-Russia Comprehensive Strategic Partnership: Formation, Features, and Prospects," *China International Studies*, July/August 2016. 67.

90. BBC News, "Russia and South Korea Spar over Airspace 'Intrusion,'" July 2019, <https://www.bbc.com/>.

91. Artyom Lukin (@ArtyonLukin), Twitter, 23 July 2019, <https://twitter.com/>, in response to Ben Westcott, Brad Lendon, and Yoojung Seo, "Warplanes from Four Countries Face Off in Asian Confrontation," *CNN World*, 23 July 2019, <https://edition.cnn.com/>.

# Strategic Choice and the Orbital Security Dilemma

LTC BRAD TOWNSEND, USA

## Abstract

The current environment in space appears to have many of the traits of a security dilemma. Left unchecked, security dilemmas create unstable conditions and generate suboptimal arms racing, potentially leading to war. The growing orbital security dilemma is being fueled by the common perception that space is an offense-dominant environment. This misperception of offense dominance is ruling out viable reassurance strategies and forcing states to pursue self-defeating policies that are only intensifying the security dilemma in space. This article addresses the more nuanced reality of the offense-defense balance in space and its implications for the future of great power competition in orbit. It concludes that states should pursue a hedging strategy that favors robust defensive capabilities and a disaggregated space architecture due to a combination of a nearly neutral offense-defense balance and the persistence of some form of the security dilemma driven by borderless orbital geography.

\*\*\*\*\*

The common refrain from US political and military leaders is that space is now a war-fighting domain just like any other.<sup>1</sup> The casual frequency of this previously taboo statement highlights the rapid shift in US space policy from seeming complacency to proactive deterrence. As the US perceives an increasing threat to its space power by strategic competitors, its policies are reflecting a more aggressive military posture in space. This stance can fuel the possibility of an arms race in orbit as other states react to US efforts to safeguard its space assets in unpredictable ways. The behavior of the major space powers in orbit is creating the conditions for the classic action-reaction-overreaction cycle described by the security dilemma that drives arms races and can often lead to tragic and unintended outcomes, especially when the perception of the military conditions varies from reality.

A security dilemma arises when a state's attempts to increase its security threaten other states, leading to unnecessary conflict or intensified

security competition.<sup>2</sup> It is a relatively simple concept with complex outcomes. Since state behavior in space is beginning to resemble one of security seeking, the security dilemma can provide a framework for explaining and predicting future outcomes. But foremost, understanding the nature of the orbital security dilemma may facilitate determining a way to preserve the current fragile peace in the space domain, a condition that best suits the desires of all spacefaring states.

Among the many drivers of this security dilemma are the heightened dependence of conventional military capabilities on space support and the growing economic importance of space. This combination of factors has revived early space age fears of war in space that until recently were slowed by a combination of norms, technical limitations, and the relatively limited value of the domain both militarily and economically. These mitigating factors that once helped maintain stability in space are rapidly disappearing. Space has become vital to the economic well-being of developed nations as well as to the ability to project military power. As the cost of space access decreases, the connection between space power and national power will strengthen, bolstering the likelihood of intense military competition in orbit.

The perception of vulnerability in space is partly driving the severity of the security dilemma and the nature of military competition in orbit. This sense of vulnerability is a function of the common understanding that the offense dominates in space and that the purpose of space systems as offensive or defensive weapons is difficult or impossible to differentiate. These perceptions, accurate or not, create the conditions for a severe security dilemma but do not mean that all the negative consequences of a security dilemma-driven arms race will occur, particularly when the conditions for the dilemma are isolated to a single domain. However, they do point to the potential expansion of security competition into an entirely new physical domain for the first time in over a century—with dangerously uncertain consequences and outcomes. A clear understanding of the offense-defense balance in space and the conditions under which it changes will allow policy makers to more accurately assess threats and vulnerabilities while allowing for the development of viable reassurance strategies. The reality is that as more satellite constellations are launched, the balance will tilt in favor of the defense—creating more opportunities for cooperation that can moderate the orbital security dilemma and preserve peace.

This article addresses the perception of military conditions in space within the security dilemma. First, it reviews the relationship between the security dilemma and the offense-defense balance. It also addresses

methods for measuring the offense-defense balance and the degree of distinguishability of space weapons. Next, the article determines the offense-defense balance in orbit at different levels of warfare. It then addresses the challenge of distinguishing between offensive and defensive space systems. Finally, this article presents a brief analysis of effective national strategies in an environment increasingly driven by the dynamics of the security dilemma.

## Security Dilemmas and the Offense-Defense Balance

The *security dilemma* is a term first used by John Herz, the influential international relations author and scholar, more than 60 years ago to describe a situation that arises in an anarchic environment where one individual or group's quest for security through the accumulation of power creates insecurity in neighboring individuals or groups.<sup>3</sup> In an effort to ensure their security, neighboring individuals or groups accumulate power in response. An action-reaction cycle then ensues, with each party attempting to ensure its security by accumulating more power than its neighbor. In an anarchic world where individuals or groups are chiefly concerned with ensuring their own security, the security dilemma provides an explanation for competition and conflict.

In his landmark article "Cooperation under the Security Dilemma," Robert Jervis lays out many of the challenges and conditions associated with understanding the severity of a security dilemma.<sup>4</sup> He highlights that there are two crucial drivers of the dilemma: the distinguishability of defensive from offensive weapons and "whether the defense or the offense has the advantage."<sup>5</sup> If defensive weapons are easily distinguishable from offensive weapons, then a state can arm itself without threatening the security of its neighbors. In addition, when the "defense has the advantage over the offense, a large increase in one state's security only slightly decreases the security of [its neighbors]."<sup>6</sup> The result of this insight is that the balance between offense and defense is a key determinant of the severity of the security dilemma. For instance, if the offense has the advantage and states cannot distinguish between the nature of weapons, then the security dilemma is "doubly dangerous."<sup>7</sup> Alternatively, if the defense has the clear advantage and weapons types and uses are distinguishable, then the situation is stable and the security dilemma ceases to be an issue (table 1). This offense-defense balance can drive status quo powers to act aggressively if offense dominance exists, or it can encourage cooperative behavior if defense dominates.<sup>8</sup>

**Table 1. Impact of offense-defense distinguishability on security dilemma**

Offense	Offensive Advantage	Defensive Advantage
Not distinguishable from defense	Doubly dangerous	Security dilemma
Distinguishable from defense	No security dilemma, though aggression possible	Doubly stable

*Adapted from Robert Jervis, "Cooperation under the Security Dilemma," World Politics 30, no. 2 (1978): 211.*

In *Causes of War*, Stephen Van Evera goes so far as to argue that the offense-defense balance can act as the centerpiece of a separate theory of international relations. The core of his argument is that shifts in the offense-defense balance, real or perceived, substantially affect the risk of war because these calculations drive "policymakers' estimates of relative power."<sup>9</sup> The result is that when conquest is easy, war is far more likely. A perception of power imbalance, coupled with the ease of conquest in an offense-dominant environment, creates fear. This fear forces states to seek increased security through alliances, arms control agreements, or the accumulation of arms.

According to Van Evera, another negative outcome of misperceptions of the offense-defense balance occurs when the offense is perceived to have the advantage. Under these conditions "states hold military secrets more tightly," allowing militaries "to monopolize information" and leaving inflated assessments of the threat unchallenged.<sup>10</sup> Van Evera's observation further reinforces the need for a clear understanding of the offense-defense balance in space. Given the highly secretive nature of military space programs and an accepted perception of offense dominance in space, his assessment has ramifications for understanding current state behavior. Is the near-monopoly by national militaries on information about actions and events in space driving a cycle of overreaction and helping to fuel the security dilemma?

The quest for power to provide security from others' power is central to Herz's original formulation of the security dilemma.<sup>11</sup> Jervis recognizes that a way to describe power is in terms of the offense-defense balance; Van Evera takes this thread to the extreme and tries to make it stand on its own as the independent variable in his own theory.<sup>12</sup> Charles Glaser, in *Rational Theory of International Politics*, argues that the offense-defense balance is still important but must be included in a broader theoretical framework to accurately capture the severity of the security dilemma.<sup>13</sup> He substantiates his argument by incorporating the offense-defense balance

into a grouping of material factors that influence the security dilemma. The material variable's impact on the severity of the security dilemma is a function of the state's power, multiplied by the offense-defense balance.<sup>14</sup> Glaser defines *power* as the "ratio of states' resources that can be converted into military assets."<sup>15</sup> This definition can be understood as referring to military capability versus purely military assets since many normally non-military space assets have military capability, such as commercial communications satellites. The concept of material power as a driver for the security dilemma is not new. It is at the core of the offensive realism school of international relations, though Glaser's nesting of the offense-defense balance within the material variable does offer additional insights when combined with other aspects of his theory. Glaser also explicitly incorporates two additional variables in his theoretical formulation of the security dilemma—motive and information—that were only implicit in the security dilemma framework as defined by Herz and others. Motive captures the security desires of a state, which can be characterized as security seeking, greedy, or a combination of the two. Greedy states have nonsecurity reasons for expansion that can include a desire to increase "wealth, territory, or prestige."<sup>16</sup> In contrast, security-seeking states are focused on protecting their current territory or wealth. These categories are not black and white; security-seeking states can appear to have greedy motives for a variety of reasons. They might desire a buffer zone, or more strategic depth, and so might seize territory or actively pursue strategies to weaken a stronger adversary to increase their security.<sup>17</sup> Almost all states naturally have at least a basic desire for security, though some desire more based on multifarious factors. It is the uncertainty that states have over the nature of their neighbors' motives that leads to the second additional variable impacting the security dilemma—information.

According to Glaser, the other independent variable necessary in determining behavior under the security dilemma is information. In this context, it denotes "what the state knows about its adversary's motives and what it believes its adversary knows about its own motives."<sup>18</sup> This concept differs from other structural theories of international relations that treat the uncertainty about states' motives as a static assumption. Instead, this factor becomes a variable for both parties. This does not mean that uncertainty cannot be eliminated; if that were so, then the security dilemma would not exist. However, using the information variable, a state might be reasonably confident that an adversary is a security-seeking state and so influence it to pursue cooperative policies with only minor levels of hedging. In contrast, if a state were highly uncertain that an adversary was a

security-seeking state, then it might decide that pursuing cooperative policies was too risky.

The other half of the information variable is what a state believes its adversary knows about its own motives. This reversal is necessary because it can lead to reaction and overreaction under the security dilemma. If state A believes that it is obvious to an adversary that it is a status quo security seeker and the adversary, state B, continues to build up arms, then state A concludes that it must be a greedy revisionist state. However, the truth may be that state B does not see state A as a security seeker, or it has a high level of uncertainty about state A's true intentions and so pursues a competitive policy to protect itself. This sequence of misperceptions was described by Jervis, but Glaser fully incorporates it into a functional theory.<sup>19</sup>

The severity of the security dilemma is therefore determined by a combination of material, motive, and informational variables working together within the rational strategic choice framework developed by Glaser. The explicit combination of these three variables explains why states sometimes pursue what would otherwise be seen as irrational policies under traditional realist structural theories. Since more than material factors impact the security dilemma in Glaser's theory as independent variables, a state might pursue cooperative policies when the material factors alone would point to competition and vice versa.<sup>20</sup> These variables combined with the offense-defense balance influence the severity of the security dilemma (table 2).

**Table 2. Severity of the security dilemma**

Motives	Offense Advantage	Defense Advantage
State is likely greedy	Very severe	Moderate
State is equally likely greedy or security seeker	Severe	Mild
State is likely security seeker	Moderate	Essentially eliminated

*Adapted from Charles L. Glaser, *Rational Theory of International Politics* (Princeton, NJ: Princeton University Press, 2010), 87.*

Determining the type and severity of a state's security dilemma is valuable in deciding whether to pursue competition or cooperation in space. This choice is influenced by the three variables mentioned above, making it a complex and difficult decision not entirely confined to the space domain. Defaulting toward cooperation seems to be the best option for escaping the security dilemma, but this is not always the case. Competing by pursuing arms can sometimes be the optimal choice for preventing war

or at least of decreasing the probability of conflict. When facing a greedy state in an offense-dominant environment, the optimal choice for a state is to pursue arms and seek to deter its adversary.<sup>21</sup> Of course, war is still more likely when a security-seeking state is faced with a greedy one, but choosing not to arm would only further increase the likelihood of conflict by encouraging the greedy state to take advantage of weakness, and so the logic of deterrence becomes dominant. The pursuit of arms for security is then the optimal choice under these conditions because cooperation would be dangerous.

In contrast, a suboptimal arms race can generate the insecurity that a state is attempting to avoid when cooperation would be a better option.<sup>22</sup> Suboptimal arms races can create dangerous uncertainty and lead to conflict. At best, suboptimal arms races are a waste of resources that a state would be better off investing elsewhere, particularly in the space domain where changes in technology can rapidly offset the advantages gained through arms racing.<sup>23</sup>

The overall logic of choosing to pursue arms or cooperation is shown in table 3, below. Both the upper left and lower right quadrants are optimal choices. In the upper left, a state's best choice was to arm to deter a greedy adversary. In the lower right, both states sought cooperation and correctly did so. In the upper right quadrant is the classic security dilemma where a state chose to arm when it did not need to, with the attendant negative impacts on its security as other states responded. The other suboptimal choice is when a state chose not to arm even when faced with a hostile adversary, leaving the cooperating state dangerously vulnerable. War is always possible with or without arms races, though it is the uncertainty inherent in the security dilemma that drives these suboptimal choices that "make war unnecessarily likely."<sup>24</sup>

**Table 3. Quality of arming decisions**

		State Should Have Armed/Raced	
		Yes	No
State Armed/Raced	Yes	Optimal Arming: Necessary Races	Suboptimal Arming: Dangerous Races
	No	Suboptimal Restraint: Dangerous Cooperation	Optimal Restraint: Desirable Cooperation

Source: Charles L. Glaser, *Rational Theory of International Politics* (Princeton, NJ: Princeton University Press, 2010), 233.

Glaser's models for the security dilemma and arming decisions do have shortcomings when applied together. The first is a 2x3 matrix of possible outcomes while the second is a 2x2 matrix of arming decisions that prevent straightforward application. Considered independently, both models



are logically consistent, but there is significant underlap when they are applied together. If conditions are such that the offense-defense balance only slightly favors the defense and a state's adversaries are equally likely to be greedy or security seekers, then it is unclear from table 3 if a policy of restraint or arming is optimal. This unclear middle ground is also the most likely to occur in applications where motivations, intentions, and capabilities become clearly defined only after the fact, and likely not even then. A realm of hedging then exists between a policy of either optimal arming or restraint. Actions under these conditions depend on the degree of distinguishability in the offense-defense balance, something that neither of the structures proposed by Glaser explicitly considers.

In another approach, Evan Montgomery places the offense-defense balance in context with the degree of distinguishability and addresses the underlap in Glaser's two models.<sup>25</sup> The focus of Montgomery's model is providing a guide for how states can reveal their benign intentions—allowing other states to clearly identify them as security seekers—which under Glaser's model would either moderate or eliminate the security dilemma. Montgomery does this by using an approach similar to Jervis's model discussed above, but in addition to a different focus, he also includes the more ambiguous case of offense-defense neutrality. The resulting matrix does not explicitly identify whether cooperation or competition is the optimal strategy for a state under the conditions identified in the model. However, in determining the cost of pursuing a cooperative policy, it highlights the risks associated with choosing restraint over competition (see table 4, next page).

The models discussed above demonstrate the close relationship between the offense-defense balance and the security dilemma. They also show the importance of striving to determine the truth of a concept as subjective as the offense-defense balance. Understanding the nature of the balance and the degree of distinguishability can point to strategies for mitigating the severity of the security dilemma in space or determining if one exists at all. Even Jervis's simple 2x2 model can lead to complex outcomes and strategies that more recent models by Glaser and Montgomery attempt to clarify. The problem is that these complex outcomes are matched by the challenges associated with accurately measuring and determining the offense-defense balance.

**Table 4. Offense-defense, reassurance, and vulnerability**

Offense-Defense Balance	Offense-Defense Differentiation	
	Yes	No
<i>Defensive advantage</i>	<ul style="list-style-type: none"> <li>• Large reductions in defensive forces are necessary to reveal benign motives.</li> <li>• Large concessions can still increase a state's vulnerability.</li> </ul>	<ul style="list-style-type: none"> <li>• Signals that decrease a state's ability to attack also decrease its ability to defend.</li> <li>• Large reductions necessary to reveal benign motives.</li> <li>• Large concessions increase a state's vulnerability.</li> </ul>
<i>Offense-defense balance neutral</i>	<p>Benign states can reveal motives without increased vulnerability because</p> <ul style="list-style-type: none"> <li>• Differentiation allows states to choose clearly defensive forces.</li> <li>• Defensive forces are as effective as offensive forces, so benign states are not at a disadvantage if they choose defense.</li> </ul>	<ul style="list-style-type: none"> <li>• Signals that decrease a state's ability to attack also decrease its ability to defend.</li> <li>• Moderate reductions in the number of forces will reveal benign motives.</li> <li>• Moderate concessions will also increase a state's vulnerability.</li> </ul>
<i>Offensive advantage</i>	<ul style="list-style-type: none"> <li>• Small limits on offensive forces sufficient to reveal benign motives.</li> <li>• Small concessions increase a state's vulnerability.</li> </ul>	<ul style="list-style-type: none"> <li>• Signals that decrease a state's ability to attack also decrease its ability to defend.</li> <li>• Small reductions in the number of forces will be sufficient to reveal benign motives.</li> <li>• Small concessions increase a state's vulnerability.</li> </ul>

*Adapted from* Evan Braden Montgomery, "Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty," *International Security* 31, no. 2 (2006): 169.

## Measuring the Offense-Defense Balance in Space

The offense-defense balance is not an easy factor to measure despite the influence it can have on military behavior, especially as it is not the reality of the balance but the perception of it prior to conflict that impacts behavior. For this space-centric discussion, the *offense-defense balance* is the ratio of the cost of offensive forces versus the cost of successfully defending against those forces without significant degradation of capability.<sup>26</sup> This definition removes any troublesome references to territory, common in most definitions but irrelevant in the space domain. Using this relative method of measurement is not without subjectivity as the cost of attacking versus the cost of defending must be categorized in subjective

terms such as low, very low, or extremely high. Complicating this subjectivity, the process and methods of measuring the offense-defense balance are extremely controversial, with some arguing that it cannot be done.<sup>27</sup> Despite this ambiguity, the perception of offensive or defensive advantage plays a central role in determining states' arming choices and behaviors and remains a fixture of modern international relations theory.<sup>28</sup>

Two of the primary factors usually cited as determining the offense-defense balance are geography and technology.<sup>29</sup> Geography is usually the least controversial factor affecting the offense-defense balance between states.<sup>30</sup> If two states share a mountainous border that is difficult to cross or are separated by an ocean, then defense would have the advantage in any conflict between those states. In space, unlike on Earth, all states suffer from the same constraints imposed by orbital dynamics, so geography affects all nations equally.<sup>31</sup> Some might argue that access to launch sites near the equator—allowing larger masses to reach geosynchronous orbits for a given mass of fuel—represents a geographic limitation that may favor some states over others. However, the difference is small enough that it is not a significant strategic factor in the offense-defense balance. For example, there is only a 22 percent gain in mass to geosynchronous orbit for a Soyuz launching from Baikonur, Russia (46 degrees North latitude), versus launching from Kourou, Guiana (5 degrees North Latitude).<sup>32</sup> While this difference is undoubtedly economically significant, it is not enough to affect the balance of military power in space between great powers and so can be disregarded.

The second primary factor that affects the offense-defense balance is technology. Since geography in space is shared among states, it becomes the sole driver of the offense-defense balance in orbit. The challenge is that space technology's rapid evolution is shifting the envelope of the possible and altering the perception of threats in space. The last decade has seen remarkable developments in space technology and an accelerating pace of innovation. These changes can be most directly attributed to the paradigm-shifting decrease in launch prices combined with the development of mass-produced small satellites that can operate in constellations. These two trends are mutually reinforcing and will lead to a proliferation of satellites in orbit over the next decade. This surge in space platforms will create challenges for the other factor that influences an assessment of the severity of the security dilemma—the degree of distinguishability.

Determining the degree of differentiation between offensive and defensive weapons is becoming increasingly difficult in space. The inability to clearly differentiate weapons systems into categories of offensive and

defensive has always presented problems, especially to attempts at arms control. Salvador de Madariaga, a Spanish diplomat, famously said that “a weapon is either offensive or defensive according to which end of it you are looking at.”<sup>33</sup> This statement highlights that the purpose of many weapons systems is dependent on how a state uses them and not on the intrinsic nature of the weapon. Even those that are explicitly defensive, such as fortifications, could be interpreted as supporting offensive purposes when they are used to free up mobile forces for duty elsewhere.

The space domain does not escape this confusion. Since space is primarily a domain for transmitting and gathering information, even a communications satellite could be construed as an offensive platform when used to support terrestrial offensive operations. To help alleviate this confusion of purpose, only the role of platforms in the space domain will be considered. Those systems that do not explicitly harm space assets are considered defensive while those designed to harm or interfere with space assets are offensive. For example, an antisatellite weapon (ASAT) or a ground-based laser is an offensive system, even if its use could be part of a defensive strategy—though this differentiation still does not entirely solve the problem of distinguishability.

The deployment of on-orbit repair and maintenance systems designed to service satellites or remove debris presents a dilemma. These systems are ostensibly designed for peaceful purposes, but a satellite with a repair arm or a net for catching debris could easily be used to damage or destroy a satellite. Unlike those explicitly offensive weapons categorized above, the purpose of these systems depends on how a state uses them. For the time being, this challenge is mitigated by the fact that only a handful of systems on orbit fall into this category. In the future, as more of these systems are launched, they will become a more pressing issue and represent a challenge to attempts at arms control agreements in space.

The issue that dual-use satellites create in determining the degree of distinguishability between space systems will be mitigated by two factors. First, the number of these systems on orbit must be constrained by the degree to which they are economically justified. The relatively small number of these platforms that could be economically justified would not allow one nation to rapidly dominate another in space. Launching a larger number of dual-use satellites than could reasonably be justified to perform their mission represents a clear provocation and an act that would clearly distinguish the specific capability as offensive. Second, while systems designed to perform commercial tasks such as repair, refueling, or debris removal can be used as weapons, they will be poor examples of them. An

analogous comparison is the military utility of commercial airliners. While airliners can be used to support military operations by transporting troops in permissive environments, they would be ineffective in comparison to dedicated military aircraft such as bombers or fighters. The technology on which commercial airliners are based could be used to develop dedicated weapons of war, but doing so requires time and experience. The fear of future dual-use commercial capabilities is largely driven by the lack of experience that humanity has with conflict in space and the implicit assumption that the offense-defense balance in space favors the attacker.

### **The Offense-Defense Balance in Space**

If a nation misperceives the offense-defense balance, it will rule out reassurance strategies that might otherwise be possible and instead default to suboptimal arming policies. Such policies are being enacted now largely due to a misinterpretation of the overall offense-defense balance. The common belief is that offense has a distinct advantage in space and that the offense and defense are indistinguishable because of the dual-use nature of many space systems. These views of offense dominance and indistinguishability are ruling out viable reassurance strategies, forcing states to pursue self-defeating policies that are further intensifying the security dilemma in space.

In the space domain, it is generally accepted that offense has the advantage. This frequently cited “fact” appears in studies, newspaper articles, and treatises on strategy—often with little support.<sup>34</sup> RAND studies cite it, as do prominent strategists such as Colin Gray who argues with some equivocation that “offense may appear to be the stronger form of war in space, given the absence of terrain obstacles, the relative paucity of capital assets (and targets), and the global consequences of military success or failure.”<sup>35</sup> Senior US policy makers also share Gray’s opinion. James Finch and Shawn Steen, the former director and deputy director, respectively, for space policy and strategy development in the US Office of the Undersecretary of Defense for Policy, argue that the domain is offense dominant because “holding space targets at risk is far easier and cheaper than defending them.”<sup>36</sup> With the notable exception of an article by Edward Ferguson and John Klein using a Clausewitzian-based premise, there are few serious attempts to refute the idea that space is offense dominant.<sup>37</sup>

It seems fairly obvious that space is offense dominant. After all, satellites are vulnerable machines. They travel in predictable orbits, and every kilogram of mass devoted to their defense leaves less available for its actual mission. The attacker is under no similar limitation and can devote all its

capabilities to defeating whatever safeguards the defender has available. Additionally, with many military satellites taking nearly a decade to design, their technology is already outdated upon launch.<sup>38</sup> During the expected 10 to 15 years of lifetime a satellite has on orbit, that technology deficit only grows with no realistic way for improvements or upgrades to occur. As a result, the attacking platform or system will almost always be newer and more capable. Even the traditional advantages of the defender do not apply. There is no terrain to leverage for a defending satellite's advantage. If orbits are terrain, then the defending satellite is essentially trapped in the orbit in which it is placed. Even if it had the fuel to move, it loses its very purpose once it changes orbit; thus, the attacker has achieved its objective merely by threatening to attack. The attacker also chooses the time and place of the attack, which can occur when the defender has limited ability to observe or react.

Another traditional defensive advantage that fails in space is that of interior lines. Interior lines traditionally allow a defender to mass forces and reinforce faster than an attacker. In space, both the attacker and defender suffer from the same physical restrictions in achieving orbit, neutralizing any advantage to either side. Finally, the bullet is always cheaper than the target, assuming that the target is not another bullet. Whatever form the attacker takes, it is optimized for a single function: destroying or disabling its target. This approach will inevitably be cheaper than the target satellite.

With all of these disadvantages accruing to the defending satellite, how can any argument be made that does not favor the offense in space? Consider the fundamental military use of space. It lies not in the individual satellite but in the ability to transmit information through it and to collect information from it. True, the satellite is critical to this process; however, the paradigm is shifting. As recently as 15 years ago, the number of satellites on orbit with service to any one region in any particular band was relatively limited. Therefore, the ability to transmit information through space and the health of the satellite were inextricably linked. In December 2019, more than 2,218 active satellites were on orbit, up from around 500 in 2008, and we are on the cusp of the era when active small satellite constellations and reduced launch costs will cause these numbers to skyrocket.<sup>39</sup> The space between orbital slots in the geostationary belt also continues to shrink with multiple satellites now operating in the same slot. With so many satellites on orbit, a hostile entity looking to interfere with a signal will first have to contend with finding the signal. Once found, whether the attacker uses kinetic means to threaten the sat-

ellite or nonkinetic means to target the signal will not matter. The signal can move elsewhere in moments, and the attacker is again left hunting for a needle in a haystack. A competent defender will be ready for interference or attack and—just as is done with terrestrial radio interference—have a preplanned alternate frequency. A clever defender will take things one step further by having a plan, when threatened, to further complicate the attacker's search by switching bands or even moving from fixed to mobile satellite services.

The intermixing of military, civil, and commercial signals from a variety of sources on commercial platforms creates a further complication for an attacker. Attacking the wrong signal or satellite can involve a third party in any conflict, an undesirable situation for the attacking entity. The level of entanglement involved in commercial platforms varies, but it creates another issue that any attacker must consider. When the array of challenges involved in the actual mechanics of preventing the transmission of information through space is considered, the offense-defense balance is more neutral than commonly thought. While the sheer number of signals on orbit makes stopping the transmission of information extremely difficult, preserving the ability to gather information is even more complex.

Gathering information from space requires a platform. Thus, the loss of a satellite could create a catastrophic loss of information-gathering ability, although this situation is changing rapidly. In 2018, there were 684 active satellites on orbit whose primary purpose was Earth observation in a variety of spectrums—nearly double the number in 2016.<sup>40</sup> While much of the growth is coming from small satellites, there is significant growth in larger satellites as well. The US-based company Planet alone now offers three- to five-meter resolution of anywhere on the globe every day, with resolutions as low as .5 meters less frequently.<sup>41</sup> This is a capability that no one, civilian or military, ever had as recently as two years ago. It is becoming very challenging for a nation to hide anything and even harder to prevent someone from gathering information. There are simply too many commercial, scientific, and national systems imaging the Earth for any attacker to completely deny them the ability to image an area.

The one area where no commercial system can yet compensate for is in dedicated systems with no civilian application, such as missile warning. Satellites performing these missions are currently irreplaceable, though their specific association with nuclear deterrence provides them with their best protection. Any attack on these systems represents an attack on a country's nuclear deterrent, with attendant consequences. However, commingling these systems with non-missile-warning conventional missions

such as “battlespace awareness” represents a dangerous trend that makes these satellites legitimate targets in any conventional limited conflict.<sup>42</sup> Whether the intent behind an attack on these satellites is a prelude to nuclear conflict or an effort to deny an enemy information, a defender must assume the worst. Even unintentional damage by debris from another destroyed satellite could be misinterpreted as an intentional attack, given the inability to directly observe the damage. Protecting this handful of expensive, vital satellites is best done by avoiding a suboptimal arms race in space.

Fundamentally, the greatest threat to a nation’s space control will be an adversary’s ability to disrupt or deny the information flow provided by a nation’s space assets, whether commercial or military. Since a larger presence on orbit makes this task more difficult, it benefits a nation to have the largest, most resilient space architecture possible. Resiliency is the ability of a nation’s assets “to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions.”<sup>43</sup> One of the easiest ways to achieve resiliency is by dispersing the capability to gather and transmit information across as many platforms as possible, commonly called disaggregation. Because the number of commercial satellites in orbit is increasing rapidly, a nation’s ability to achieve resiliency through disaggregation will depend on the size of its commercial space industry. However, commercial providers are unlikely to offer the necessary level of conflict protection for their satellites due to the additional costs. This reluctance means that while the individual satellites may be more numerous, they are also more vulnerable to interference or other forms of attack.

Where then does the offense-defense balance lie? The individual satellite remains vulnerable to attack and nearly impossible to defend. Therefore, at the level of the individual satellite—the tactical level of space—the advantage does lie with the offense. At the level of a constellation of similar platforms, a signal can move or one platform can compensate for the loss of another, but the target set remains limited to a subset of satellites. A smaller constellation favors the attacker while a larger, more robust constellation can shift the advantage to the defender. The balance at this level—the operational level—is then generally neutral depending on the number of satellites and the ease with which they can be replaced. At the strategic level, where the balance is measured against the aggregate ability of a nation to transmit and gather information using space, the balance begins to shift in favor of the defender (table 5). As long as a nation can maintain access to a significant share of the commercial market, it is un-



likely that another nation can entirely deny it the use of space. Space is an environment where nations can always disrupt and degrade the capabilities of other nations. However, one nation cannot entirely deny another the ability to substantially leverage space as long as a neutral commercial market exists.

**Table 5. Offense-defense balance in space**

Level of War		Balance
Tactical:	Individual satellite	Strongly favors offense
Operational:	Constellation or specific architecture	Neutral depending on constellation size and architecture resiliency
Strategic:	Continued national access and ability to exploit space	Slightly favors defense

### Distinguishability

Determining the need for competitive or cooperative policies in space also requires determining the distinguishability between the offense and the defense. This task is notoriously difficult as most weapons are not intrinsically either offensive or defensive. Instead, it is the intent behind the weapon that determines its nature. While some space systems are more easily distinguishable than their terrestrial counterparts, others suffer from the same degree of confusion. Space also has norms of behavior established at the outset of the space race that differ from any other domain and significantly affect distinguishability in space and the degree of uncertainty that comes from dual-use systems.

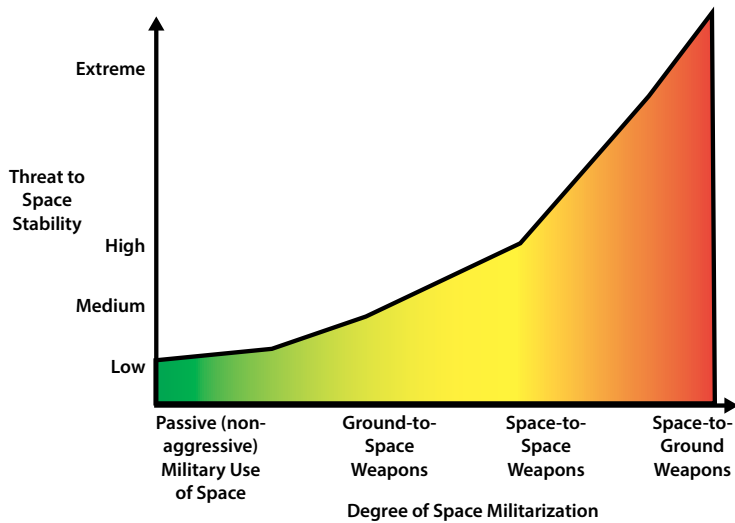
Before establishing the degree of distinguishability in space, clarification on degrees of space militarization is necessary. Since the very beginning of the space age, the US has publicly supported the peaceful use of space while at the same time quietly steering the definition of *peaceful* toward “the non-aggressive use of space.”<sup>44</sup> The Eisenhower administration saw the unique benefits of space-based reconnaissance in verifying Soviet military capabilities and preserving the peace between the two superpowers. The precedent established of defining *passive military use* as peaceful has continued, even as the passive use of space moved beyond reconnaissance and treaty verification. Today, passive systems—such as satellite communications and GPS—actively contribute to offensive military actions on the ground, yet they remain classified as passive and therefore peaceful systems. Intentionally conflating *nonaggressive* with *peaceful* from the outset established a unique domain norm that remains in effect

today. In any other domain, a system that provides targeting data to weapons systems would clearly be a legitimate military threat, yet space maintains a definition of *peaceful* based on a precedent only tacitly agreed to during the Cold War.

The next degree of space militarization is ground-to-space weapons. These were among the first space weapons developed and have existed in one form or another since nearly the beginning of the space age, albeit in limited numbers. ASATs are the classic example of these type of systems, which can also include ground-based jammers and lasers designed to degrade or damage orbiting satellites. The current arms race in space is focused on developing these capabilities, and the further testing and development of these weapons is an area of significant concern.

The next level of space militarization is space-to-space weapons. This category includes satellites designed to destroy or disable other satellites. Satellites designed to protect other satellites through offensive action would also fall in this category, one that is only just beginning to develop. Weapons at this level of militarization would be a dangerous new development in space. Even so, they would be a threat only to other space systems and remain within the information-centric space power paradigm mentioned earlier.

The final and most dangerous level of space weaponization is the fielding of space-to-ground weapons (fig. 1). No nation has crossed this proverbial Rubicon, though if it does happen, it will create a dangerously unstable situation. The advent of space-to-ground weapons would invalidate information-centric space power theories because preserving the ability to gather and transmit information through and from space would no longer solely define the military utility of the domain. These space-to-ground weapons could provide nuclear effects without nuclear fallout from orbits low enough that they would give the defender minimal reaction time. Unlike ICBM launches that are easily detectable, space-to-ground weapons would most likely have much lower launch signatures.<sup>45</sup> These launch platforms would individually be vulnerable, and an opponent would no doubt develop ASATs designed to attack them. Both nations in this situation would enter a dangerous offense-dominant environment with extremely low crisis stability. In essence, if a situation developed that increased tensions, each nation may find itself in a use-it-or-lose-it quandary. This first-strike instability would pressure leaders “to strike first in a crisis to avoid the worst consequences of incurring a first strike.”<sup>46</sup> Thankfully, this paradigm shift is not on the immediate horizon, though many believe it is inevitable.



**Figure 1. Degree of militarization and threat to space stability.** (Note: Values are for illustrative purposes only and not based on empirical analysis.)

With the degrees of space militarization delineated, it is now possible to return to the issue of determining the degree of distinguishability. Established norms determine what constitutes the peaceful use of space, and since *peaceful/nonaggressive* and *defensive* are nearly synonymous terms in an environment dependent on information, anything designed to gather or transmit information is distinguishable as nonoffensive. This established norm of passive military use is stretched by the dependence that conventional offensive military capabilities have on space, yet it still holds. Nonetheless, the very dependence of conventional forces on these capabilities makes space capabilities a tempting target and drives nations to develop weapons designed to attack satellites. The next tier of militarization, ground-to-space, is where challenges of distinguishability begin. Anti-ballistic missiles (ABM) and ASATs are the most obvious examples of systems that suffer from distinguishability problems at this level. As discussed previously, a system designed to destroy or disable ballistic missiles can easily be retargeted to strike satellites in low orbit. A dedicated ASAT is only distinguishable from an ABM if it is designed to travel to altitudes beyond which ballistic missiles travel. Even if an ASAT and a missile defense system can be distinguished, the ASAT system might be a justified defensive system if there exists a legitimate reason to suspect that an adversary has placed weapons on orbit. The ASAT system then becomes indistinguishable in purpose from other weapons as it could be used defensively to deter enemy threats or offensively to attack peaceful satellites.

Other systems in this tier include ground-based lasers and jamming systems. These systems might have reversible effects, or they may cause permanent damage to the target. The intent of these systems could vary and may include causing interference with reconnaissance or navigation satellites assisting with enemy targeting. While this usage would be considered defensive in most contexts, any system designed to attack satellites for any reason can be classified as offensive. This simplistic categorization is only possible due to the established norms that passive satellites are peaceful. Therefore, any attack for any reason against passive satellites falls into the category of offense. This implicit understanding is present in US doctrine, which describes *offensive space control* as involving “measures [to] deceive, disrupt, degrade, deny or destroy space systems or services.”<sup>47</sup> US doctrine makes no allowance for the intent behind why negation of enemy systems may be occurring, simplifying the categorization of ground-to-space weapons outside of ABMs as offensive.

The discussion of intent does enter into the equation when evaluating the distinguishability of defensive systems on orbit. The same US doctrine describes *defensive space control* as “all active and passive measures taken to protect friendly space capabilities from attack, interference, or unintentional hazards.”<sup>48</sup> The inclusion of active defense in this description leads to confusion of intent. According to this doctrine document, *active space defense* “consists of those actions taken to neutralize imminent space control threats to friendly space forces and space capabilities.”<sup>49</sup> In this definition, usage of the term “imminent” seems to clarify any confusion over what active defense is; however, what constitutes an imminent threat is not defined. Could a satellite belonging to a hostile nation sharing the same orbit be an imminent threat? Or does the satellite have to take aggressive action such as approaching within a given distance of a friendly satellite? If the friendly satellite possesses a defensive system capable of disabling the approaching satellite, could that system be used for offensive purposes? Lack of clarity with regard to defining imminent threats blurs the line between offensive and defensive space control.

It is under these conditions that the secrecy surrounding military satellite capabilities becomes an issue. While the orbits and designations of military satellites are generally known, the purposes of these platforms are impossible to verify. Unlike terrestrial weapons systems that can be easily imaged and observed in use, it is nearly impossible to verify that if a nation claims to launch a communications satellite, it is not instead launching a weapons platform or intelligence asset. The US Air Force recognized this problem and revealed a previously classified program in 2014 designed to

image satellites in geosynchronous Earth orbit (GEO).<sup>50</sup> The purpose of revealing this program, according to Gen William Shelton, was to “discern when adversaries attempt to avoid detection and to discover capabilities they may have which might be harmful to our critical assets at these higher altitudes.”<sup>51</sup> Imaging adversary satellites can clarify a satellite’s purpose, but the distance between two satellites in GEO may be tens of thousands of kilometers and thus prevent timely close inspection. Even if a close approach is made, the adversary satellite may possess the outward characteristics for its stated purpose while housing offensive weapons. Since military satellites are not available for general use, there is no way to verify that a particular satellite can, in fact, perform its stated mission even with visual inspection.

The ability to image satellites offers some reassurance, but space is large, and launch platforms can orbit multiple satellites simultaneously. The Indian space agency holds the current record for a multiple satellite launch, with 104 satellites of various sizes launched at once in 2017.<sup>52</sup> Each time a nation launches a military satellite, the possibility exists that the official payload is not the only payload on board. An exquisite level of space situational awareness is required to ensure that no additional satellites are on board. If they are small enough, these additional payloads may disguise themselves as launch debris to escape detection.

A Russian launch in 2014 attempted this trick of hiding in the debris. Following the launch of three Russian Rodnik military communications satellites, a piece of supposed debris from the launch began maneuvering.<sup>53</sup> The object was not part of the official Russian launch declaration, and speculation on its purpose and nature ranged from experimental repair vehicle to hunter-killer satellite. Whatever the cause, it demonstrated the ease with which nations can add additional payloads to launches without declaring them, hoping to evade detection. The US has the best space tracking network of any nation, and even it has substantial weaknesses that could easily allow something like this Russian action to go unnoticed.<sup>54</sup> Nations with much less robust tracking networks than the US can only rely on the data the US chooses to share about its satellites’ purposes and capabilities, leaving significant room for suspicion and uncertainty of the type that fuel security dilemmas. With the rapidly growing number of satellites on orbit, it will be increasingly difficult to verify that every military satellite is what it is purported to be.

Military satellites are not the only ones that suffer from issues of distinguishability. While commercial communications, weather, and reconnaissance satellites create little suspicion because they are performing their

intended purpose daily for a variety of users, other commercial satellites, by their very design and nature, create suspicion. Commercial or civil ventures designed to refuel satellites, repair them, or remove debris can easily be used to damage or disable other satellites. For example, in 2018 Chinese researchers proposed a space-based laser designed to remove space debris from orbit.<sup>55</sup> This ostensibly civil research program would involve a satellite with a laser designed to heat targeted debris and deorbit it. A satellite mounting a laser designed to remove debris would have obvious dual-use potential and could serve as a test bed for future space-based weapons. This proposal is just one of many attempting to deal with the problem of space debris, and any of them could easily be used to destroy active satellites. The one mitigating factor is that at this time such satellites are only in the earliest stages of development and testing.

Among existing satellites and space systems, distinguishability is high relative to other fields of military endeavor. The establishment of norms early in the space era that information gathering and transmission, even in support of military efforts, are nonaggressive and peaceful greatly aids distinguishability in space. This differentiation makes ground-to-space weapons designed to interfere with satellites inherently offensive. Some confusion of intent does exist regarding active defenses on orbit and dual-use commercial systems. However, it is mitigated by the relative lack of known systems with these capabilities. One complicating factor is the uncertainty over the true purpose of military satellites. Distinguishability among military platforms is highly dependent on whether the satellite that a nation claimed it launched was in fact the one it did launch. The Russians have shown that hiding potential orbital weapons among launch debris is possible. Even with this caveat, distinguishability remains relatively high among existing space systems.

### **Cooperation or Competition**

Returning to Jervis's interpretation of the impact of the offense-defense balance on the security dilemma leaves us with no clear answer for its current severity or a way to escape it. While distinguishability is relatively high among space systems compared to other military domains, the offense-defense balance is not nearly as apparent. It does not obviously favor the offense when an observer expands their viewpoint beyond the individual satellite to consider the capability provided by a constellation of platforms. The balance can best be described as generally neutral with a slight tilt in favor of the offense. This balance will shift to neutral with a

slight tilt in favor of the defense as more satellite constellations are launched into low Earth orbit over the next decade.

Relying on Jarvis's 2x2 matrix of possibilities, this combination of offense-defense balance and distinguishability indicates that no security dilemma should exist in space but that aggression in space is possible. This conclusion does not seem to match current rhetoric or actions on orbit. Perhaps because the reality does not matter, the perception of the balance prior to conflict is the defining factor in determining behavior. The current perception of these factors places the great space powers in a doubly dangerous security dilemma according to the model developed by Jarvis.

The usage of the offense-defense balance by Glaser to measure the severity of the security dilemma is more informative than Jarvis's 2x2 model in that it provides for more gradations within the dilemma. If a minor offensive advantage exists, then some form of security dilemma also exists that can range from moderate to severe. As the advantage shifts toward the defensive, the security dilemma will moderate but is only eliminated if no uncertainty exists about the intentions of other states as security seekers. This event is unlikely to occur because space suffers from a multistate dilemma driven by the shared geography of space.

Orbital dynamics means that all states share a common border in space, so the actions of one state affect all states. The unique nature of the space domain means that the strategic choices that a state makes must be suitable for all the nations with a presence in the domain. In space, a state will find it difficult to pursue restrained arming policies centered on cooperation with one adversary while also deterring another potential adversary given the shared nature of orbits. The implication is that a state will find it increasingly difficult to determine if space-capable nations are security seekers based on the information it has about their motives and intentions. At best, a state can conclude that its potential adversaries are equally likely to be either greedy or security seekers. Using Glaser's model, this incertitude indicates that a severe or very severe security dilemma exists in space. Even if the balance shifts slightly in favor of the defense, a moderate or mild dilemma will persist due to the multistate dilemma in space.

States are not entirely passive actors subject to the conditions of the security dilemma. Understanding the offense-defense balance allows states to choose strategies that can help moderate the dilemma, as indicated by Montgomery's model. Using this model, current conditions in space can best be typified by a neutral balance with differentiation. This characterization implies that defensive strategies are as effective as offensive ones, so a state can choose a defensive strategy without leaving itself

too vulnerable. By choosing a defensive strategy, a state will signal benign intent and clearly identify itself as a security seeker. Doing so gives other states information that can help them more confidently determine that other states are security seekers and allows them to avoid suboptimal arming and moderate the security dilemma.

## **Conclusion**


The perception of the balance and degree of differentiation can substantially impact the security dilemma and drive decisions on arming in space. Even with a more nuanced understanding of the balance, it is difficult to make a definitive recommendation against pursuing arms in space. Cooperation among states in space has significant benefits in that it avoids unnecessary suboptimal arming. However, the possibility that at least one space power has greedy motives is high, so pursuing a policy of restraint in space could leave a nation that is dependent on space dangerously vulnerable. If this uncertainty means that states default to competitive policies in space, then the real question is whether it is possible to pursue defensive capabilities and moderate the security dilemma in orbit. Given the status of the offense-defense balance and the ability to somewhat differentiate systems by function, a defensive posture on orbit seems to be the best compromise approach for preserving capability while promoting cooperation.

Relying on the limited number of factors considered in this article, it seems that the optimal policy is some form of defensive arming. During the Cold War, some degree of restraint and cooperation was possible due to fewer actors in space and less dependence of conventional military capabilities on space assets. As more nations enter the space domain, the ability to adopt cooperative stances on orbit will only grow more difficult. The combination of a nearly neutral offense-defense balance and the persistence of some form of security dilemma indicates the prudence of pursuing a hedging strategy in favor of robust defensive capabilities and a disaggregated space architecture.

A caveat to the conclusion above is that the offense-defense balance and the degree of distinguishability in space are not static. The ongoing proliferation of small satellite constellations will increasingly shift the overall balance in favor of the defense. This beneficial trend will be countered by decreasing distinguishability between offensive and defensive capabilities on orbit driven by the proliferation of dual-use systems designed for a variety of legitimate purposes. Decreasing distinguishability will create misperceptions of intent as defensive actions are far more likely to be mistaken as aggressive. As this trend continues, the value of pursuing



a robust defensive posture will increase. In the future, the likelihood of unintended conflict in space will grow even as the overall defensive shift in the offense-defense balance increases the possibility of successful multi-state cooperation.

The danger is that without a clearer understanding of the true vulnerability of space systems among policy makers and military personnel, a cycle of action-reaction-overreaction is likely to occur in the current space environment. This cycle may generate an intensifying arms race that could lead to suboptimal arming, wasteful spending, and unnecessary tension between space powers. Understanding the nuanced nature of the offense-defense balance allows for a more constrained approach to arming in orbit, which can inform future strategy decisions and moderate the orbital security dilemma—decreasing the possibility of future conflict in space. 

#### **LTC Brad Townsend, USA**

LTC Brad Townsend, US Army, is the author of the forthcoming book *Security and Stability in the New Space Age: Alternatives to Arming* (Routledge Press, 2020). He holds a PhD and MPhil in military strategy from the US Air Force's Air University School of Advanced Air and Space Studies. A 2002 graduate of the US Military Academy, he also earned an MS in astronautical engineering from the Air Force Institute of Technology and an MS in space operations management from Webster University. He currently serves as a space policy advisor on the Joint Staff.

#### **Notes**

1. Statements to this effect have been made in public forums by almost all senior administration officials from President Trump downward beginning with Air Force Secretary Heather Wilson's testimony to the SASC in 2017. Marcia Smith, "Top Air Force Officials: Space Now Is a Warfighting Domain," 17 May 2017, <https://spacepolicyonline.com/>.
2. Evan Braden Montgomery, "Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty," *International Security* 31, no. 2 (Fall 2006): 151.
3. John H. Herz, "Idealist Internationalism and the Security Dilemma," *World Politics* 2, no. 2 (1950): 157.
4. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214.
5. Jervis, 186–87.
6. Jervis, 187.
7. Jervis, 211.
8. Jervis, 188.
9. Stephen Van Evera, *Causes of War* (Ithaca, NY: Cornell University Press, 1999), 13.
10. Van Evera, 13–14.
11. Herz, "Idealist Internationalism and the Security Dilemma," 157.
12. See Jervis, "Cooperation under the Security Dilemma"; and Van Evera, *Causes of War*.

13. Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton, NJ: Princeton University Press, 2010), 3.
14. Glaser, 78.
15. Glaser, 76.
16. Glaser, 36.
17. Glaser, 36.
18. Glaser, 3.
19. See Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 62–86.
20. Glaser, *Rational Theory of International Politics*, 73.
21. Glaser, 236.
22. Glaser, 231–32.
23. Glaser, 232.
24. Glaser, 229.
25. Montgomery, “Breaking Out of the Security Dilemma.”
26. Charles Glaser and Chaim Kaufmann attempted to develop a method of measuring the offense-defense balance in an effort to apply it as an independent theory as proposed by Van Evera. Before doing so, they had to first settle on a definition of the *offense-defense balance*. They defined it as the “ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender’s forces.” Using this definition, they had some success in measuring the offense-defense balance, though they still encountered great difficulty. See Charles L. Glaser and Chaim Kaufmann, “What Is the Offense-Defense Balance and Can We Measure It?,” *International Security* 22, no. 4 (Spring 1998): 64, <https://www.jstor.org/>. Their efforts faced significant criticism of methodology as well as of the territorial focus of their definition, given that many wars are won or lost based on a single battle or raiding strategy or through other means, rather than directly by the conquest of territory. The offense-defense balance as a stand-alone theory also required the assumption that states would act optimally so that military doctrine and force deployments would not impact the balance. While an important influencing factor in determining the severity of the security dilemma, the offense-defense balance is not the sole influencing factor on state behavior and, as a result, is too parsimonious to stand as an independent theory. However, it can still provide a useful way of measuring the severity of a security dilemma and point to potential reassurance strategies for escaping it.
27. James W. Davis, Jr., et al., “Taking Offense at Offense-Defense Theory,” *International Security* 23, no. 3 (1998): 186–87, <https://www.jstor.org/>.
28. See Glaser, *Rational Theory of International Politics*.
29. Jervis, “Cooperation under the Security Dilemma,” 194.
30. Glaser and Kaufmann, “What Is the Offense-Defense Balance and Can We Measure It?,” 64.
31. This in effect removes one of the larger complaints by some (see Keir Lieber) about the nonsystemic nature of the offense-defense balance due to the fact that geography under traditional definitions impacts each state uniquely.
32. “R-7/Soyuz Data Sheet,” Space Launch Report, accessed 23 August 2018, <http://www.spacelaunchreport.com/>.
33. Quoted in Jervis, “Cooperation under the Security Dilemma,” 201.
34. See Forrest E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (Santa Monica, CA: RAND Project Air Force, January 2010), 2, <https://>

www.rand.org/; James P. Finch and Shawn Steene, "Finding Space in Deterrence," *Strategic Studies Quarterly* 5, no. 4 (2011): 11, <https://www.airuniversity.af.edu/>; and Paul Scharre, "The US Military Should Not Be Doubling Down on Space," *Defense One* (blog), 1 August 2018, <https://www.defenseone.com/>.

35. Colin S. Gray, *Weapons Don't Make War: Policy, Strategy, and Military Technology* (Lawrence, KS: University Press of Kansas, 1993), 14–15.

36. Finch and Steene, "Finding Space in Deterrence," 11.

37. Edward Ferguson and John Klein, "The Future of War in Space Is Defensive," *Space Review*, 19 December 2016, <http://www.thespacereview.com/>.

38. Cristina T. Chaplain, Director, Acquisition and Sourcing Management, US Government Accountability Office, *Space Acquisitions: DOD Continues to Face Challenges of Delayed Delivery of Critical Space Capabilities and Fragmented Leadership; Testimony before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. Senate* (Washington, DC: US Government Accountability Office, 2017), 1, <https://www.gao.gov/>.

39. Union of Concerned Scientists (UCS), "UCS Satellite Database," 1 May 2018, <https://www.ucsusa.org/>.

40. "Earth Observation Satellites in Space in 2018?," Pixalytics, 5 September 2018, <https://www.pixalytics.com/>.

41. "Planet Imagery and Archive," Planet, accessed January 2020, <https://www.planet.com/>.

42. Lockheed Martin, "SBIRS: Missile Defense Early Warning Satellite," fact sheet, PIRA SSS201608034, 2017, <https://www.lockheedmartin.com/>.

43. Air Force Space Command, *Resiliency and Disaggregated Space Architectures*, white paper (Peterson AFB, CO: Air Force Space Command, 14 April 2016), 4, <https://www.afspc.af.mil/>.

44. Note that the administration did regularly have to tamp down on USAF enthusiasm for seizing the high ground. See "Draft Position Paper for UN Ad Hoc Committee on Peaceful Uses of Outer Space: Legal Problems Which May Arise in the Exploration of Space" (White House Office of the Staff Secretary: Records, 1952–61, 22 April 1959), 8, Box 24, Space Council (7), Eisenhower Library.

45. US Air Force, "Defense Support Program Satellites," fact sheet, 23 November 2015, <https://www.af.mil/>.

46. Glenn A. Kent and David E. Thaler, *First-Strike Stability and Strategic Defenses: Part II of a Methodology for Evaluating Strategic Forces* (Santa Monica, CA: RAND Corporation, October 1990), xviii, <https://www.rand.org/>.

47. Joint Publication (JP) 3-14, *Space Operations*, 2018, II-2, <https://www.jcs.mil/>.

48. JP 3-14, II-2

49. JP 3-14, II-3.

50. Amy Butler, "USAF Space Chief Outs Classified Spy Sat Program," *Aviation Week*, 21 February 2014.

51. Gen William Shelton quoted in Irene Klotz, "US Air Force Reveals 'Neighborhood Watch' Spy Satellite Program," Reuters, 22 February 2014, <https://www.reuters.com/>.

52. Samantha Mathewson, "India Launches Record-Breaking 104 Satellites on Single Rocket," *Space.Com*, 15 February 2017, <https://www.space.com/>.

53. Sam Jones, "Object 2014-28E – Space Junk or Russian Satellite Killer?," *Financial Times*, 17 November 2014, <https://www.ft.com/>.

54. Brian Weeden, "Space Situational Awareness Fact Sheet," Secure World Foundation, May 2017, <https://swfound.org/>.
55. Kyle Mizokami, "China Proposes Orbiting Laser to Combat Space Junk," *Popular Mechanics*, 20 February 2018, <https://www.popularmechanics.com/>.

# Strategic Contours of China's Arms Transfers

MICHAEL RASKA  
RICHARD A. BITZINGER

## Abstract

Over the past two decades, China has gone from being a significant importer of conventional arms to being an increasingly competitive exporter of major weapons systems. Its increasing presence on global arms markets reflects the relative progress of Chinese defense, science, technology, innovation, and industry in terms of developing and manufacturing relatively advanced military platforms and technologies. China aims for relative parity with the global military-technological state-of-the-art base by fostering indigenous innovation—mitigating foreign dependencies on technological transfers and arms imports—while leveraging civil-military integration to overcome entrenched barriers to innovation. At the same time, China's current arms export strategy reflects varying “competitive” paths. In the developing countries of Latin America, Africa, and even Central Asia, China is trying to position itself as an alternative to Russian arms exports while also counterbalancing the influence of Western powers. Consequently, China has a growing capability to shape the direction and character of the varying regional arms competitions—not only through its military-technological development and diffusion of arms exports but, more importantly, through its strategic choices that influence the development of strategic alliances and balance of power in different geographic areas.

\*\*\*\*\*

China's rising global geopolitical aspirations—backed up by growing economic clout—shape the direction and character of its military-technological choices, including its strategic interests to strengthen its position on global arms markets. Since 2010, China has been able to accelerate its transition from a large arms importer into a net exporter, with the potential to become one of the world's leading arms exporters. Specifically, Chinese defense companies are increasingly expanding bids for weapons contracts that include missiles, armored vehicles,

artillery, ships, air defense systems, and unmanned aerial vehicles (UAV). These solicitations often align with or complement Beijing's economic, trade, and military-technical cooperation packages with select countries in Asia, Africa, and the Middle East. While China remains a net importer of advanced military technologies and components such as aircraft engines, naval weapons, and sensors, it has been able to enter new markets particularly by way of low cost, affordable service, lack of geopolitical strings, and upgrade packages.<sup>1</sup> Indeed, Chinese weapons can now be found in the armaments of Saudi Arabia, Morocco, Venezuela, Ecuador, Peru, Mexico, Nigeria, Kenya, Thailand, Turkmenistan, and Kazakhstan. How has China accomplished this transition? What factors have shaped China's arms export strategy, and ultimately, what are key strategic implications of its growing presence in the global arms market?

This article provides brief contours of China's evolving arms export strategy, its defense industry capabilities, and the impact of Chinese arms transfers on other arms-exporting nations. The principal argument is that Chinese entrance into the global arms markets is based on three major developments. First, China's defense science, technology, and industrial (DSTI) system has been gradually improving in terms of developing and manufacturing new, relatively advanced military platforms and technologies that increasingly meet the widening operational requirements of the People's Liberation Army (PLA). These include the introduction of next-generation supercomputers; aviation prototypes such as the J-16, J-20, J-31, new helicopters, and UAVs; and the ongoing construction of a second aircraft carrier, as well as record numbers of commissioned ships such as Type 054A frigates, 056 corvettes, and 052C destroyers. The constant imperative to advance the PLA's military equipment capabilities has been a long-term driver of the Chinese defense industry and its continuing reforms.

Second, China's growing position in international arms markets, including its arms export abilities, is propelled by the continuing growth of its military expenditures. From the late 1990s to 2013, China experienced double-digit real (i.e., after inflation) growth in defense spending nearly every year. In recent years, China's budget growth rate slowed, falling to 7.5 percent in 2019. However, China has moved up to become the second-largest defense spender in the world, outstripping Japan, France, Russia, and the United Kingdom; only the United States currently spends more on defense. Consequently, greater resources have been available to underwrite China's armaments production and technology acquisition—especially foreign technologies—significantly affecting the growth and modernization of the Chinese military-industrial complex and therefore

arms-exports abilities. According to a report by the International Institute of Strategic Studies (IISS), “since 2014, China has launched more submarines, warships, principal amphibious vessels and auxiliaries than the total number of ships currently serving in the navies of Germany, India, Spain, Taiwan, and the United Kingdom.”<sup>2</sup> In other words, “China’s dramatic and continuing expansion in defense spending has meant more money for innovation, more money for R&D, more money to increase procurement (and therefore production runs), and more money to upgrade the defense industrial base with new tools, new computers, and new technical skills.”<sup>3</sup>

And third, China’s advancing position in global arms markets reflects its growing global geostrategic interests and expectations of a “new era” of intensifying strategic competition and major shifts in the global security environment.<sup>4</sup> In this context, China is gradually positioning its arms exports as an instrument of its foreign policy to project presence, power, and influence in areas vital to its interests, such as South and Southeast Asia. Promoting Beijing’s Belt and Road Initiative (BRI) is one way China deepens economic links with developing regions. At the same time, China’s arms export strategy aims to provide an alternative option to markets traditionally dominated by Russian arms exports to select countries in Latin America, Africa, and even Central Asia.

### **Improving Defense Industrial Strategy**

The Chinese DSTI base has undeniably advanced over the past decade and a half in terms of developing and manufacturing new, relatively modern military systems that increasingly meet the widening operational requirements of the PLA. Its progress has reflected Chinese military modernization strategy in a “double construction” approach of mechanization and “informatization” to concurrently upgrade and digitize the PLA.<sup>5</sup> This “two-track” approach has called for both the near-term “upgrading of existing equipment combined with the selective introduction of new generations of conventional weapons”—a so-called modernization-plus approach—together with a longer-term “transformation” of the PLA along the lines of the information technologies-led revolution in military affairs.<sup>6</sup>

In the process, China’s long-term strategic military-technological programs are deeply integrated with its advancing civilian science and technology base, which has been concurrently linked to global commercial and scientific networks.<sup>7</sup> Thus, China is continuously benchmarking emerging technologies and similar high-tech, defense-related R&D programs in the United States, Russia, India, Japan, Israel, and other countries.<sup>8</sup> The key aim is to accelerate China’s “absorptive capacity” to recognize, assimilate,

and utilize external knowledge in the development of China's advanced technologies in both civil and military domains.<sup>9</sup> China calls this strategy "indigenous innovation"—first set in the 2006–20 "Medium- and Long-Term Plan on the Development of Science and Technology" (MLP).<sup>10</sup> By pursuing indigenous innovation, China aims to circumvent the costs of research, overcome international political constraints and technological disadvantages, and leapfrog China's defense industry by leveraging the creativity of other nations. Doing so includes exploitation of open sources, technology transfer and joint research, the return of Western-trained Chinese students, and, of course, industrial espionage—both traditional and, increasingly, cyber exploitation (i.e., systematic hacking).<sup>11</sup>

Notwithstanding these efforts, however, the Chinese arms industry still appears to possess only limited indigenous capabilities for cutting-edge defense R&D. Western armaments producers continue to outpace China when it comes to most military technologies, particularly in areas such as propulsion (aircraft/missile engines), navigation systems and defense electronics, and high-end composites. In retrospect, the confluence of historical legacies of centralized planning coupled with segmented technological, institutional, and management deficiencies—such as overlapping planning structures, widespread corruption, bureaucratic fragmentation, quality control, manufacturing inefficiencies, and process standardization—have precluded the Chinese military-industrial conglomerates from leaping ahead on the innovation ladder. Most importantly, no real internal competition exists, and the industry lacks sufficiently capable R&D and capacity to develop and produce highly sophisticated conventional arms. Confronting these challenges, China has progressively introduced a series of medium- and long-term defense industrial strategies, plans, and institutional reforms that have generally set two broad strategic objectives known as the "two gaps":<sup>12</sup>

- To catch up with the global military-technological state-of-the-art base by fostering "indigenous innovation," thus mitigating foreign dependencies on technological transfers and arms imports while leveraging civil-military integration (CMI) to overcome entrenched barriers to innovation.
- To provide advanced weapons platforms, systems, and technologies that would enable the PLA's transformation into a fully "informatized" fighting force—one capable of conducting sustained joint operations, military operations other than war, and missions related to



China's strategic deterrence to protect China's core national security interests beyond national borders.<sup>13</sup>

Under Xi Jinping, China's strategy to resolve both gaps has focused principally on upgrading civil and military convergence.<sup>14</sup> In particular, since 2003, the conceptual umbrella for leveraging CMI became known as Yujun Yumin—"locating military potential in civilian capabilities," signifying transfer of commercial technologies to military use and calling upon the Chinese arms industry not only to develop dual-use technologies but also to actively promote joint civil-military technology cooperation. Yujun Yumin has been prioritized in the 2004 Defense White Paper, subsequent Five-Year Defense Plans, as well as the 2006–20 MLP.<sup>15</sup> Select dual-use technology development areas, for example, include microelectronics, space systems, artificial intelligence, new materials (such as composites and alloys), propulsion, missiles, computer-aided manufacturing, and particularly information technologies.<sup>16</sup> Initially, China's political establishment envisioned CMI as institutional arrangements, paving the way for a new round of associated management reforms for the defense industry—including allowing select civilian private-sector firms to engage in defense work. These in turn would enable expanding linkages and collaboration between China's military-industrial complex and civilian high-technology R&D sectors.

In 2016, however, President Xi Jinping elevated CMI into a national-level strategy,<sup>17</sup> noting that "the integration of civilian and defense development will involve multiple fields and enable economic progress to provide a 'greater material foundation' for defense construction, while the latter offers security guarantees for the former."<sup>18</sup> In other words, CMI has been projected not only as a key enabler to the PLA's military-technological modernization, but more importantly, as a strategy for China's long-term sustainable growth, efficiency, and productivity gains. Further, the PLA views it as potentially mitigating internal socioeconomic and environmental challenges. Currently, CMI as a national strategy expands the integration of state-owned defense research, development, and manufacturing enterprises; government agencies under the State Council; universities; and private sector firms in order to advance the PLA's military modernization while supporting China's economic growth.<sup>19</sup> In this context, China created new agencies in 2017 such as the Central Commission for Integrated Military and Civilian Development and the Scientific Research Steering Committee, both tasked to advance the R&D of state-of-the-art weapons platforms and systems.<sup>20</sup>

At the same time, China's CMI places strategic importance on foreign acquisition of dual-use technologies, resources, and knowledge in selected priority areas identified in recent defense science and technology plans, such as the "13th Five-Year Defense Science and Technology Industry Plan," "Defense Science and Technology Industry 2025 Plan," and the "Made in China 2025" advanced manufacturing plan."<sup>21</sup> According to the 2015 *China's Military Strategy*, "China will work to establish uniform military and civilian standards for infrastructure, key technological areas and major industries [and] explore the ways and means for training military personnel in civilian educational institutions, developing weaponry and equipment by national defense industries and outsourcing logistics support to civilian support systems."<sup>22</sup>

### **Assessing the Impact of Chinese Arms Transfers**

According to recent data by the Stockholm International Peace Research Institute (SIPRI), Chinese exports of major arms increased by 74 percent between 2012 and 2016, and China's share of global arms exports rose from 3.8 to 6.2 percent—making it the third-largest supplier in the world, following the United States and Russia. The geographic spread and number of recipients of Chinese weapons exports have also increased. From 2012 to 2016, China delivered major arms to 44 countries—more than 60 percent of China's exports went to Pakistan, Bangladesh, and Myanmar, and another 22 percent went to Africa. China also delivered major arms to ex-Soviet states for the first time, including the 2016 delivery of HQ-9 (FD-2000) surface-to-air missile (SAM) systems to Turkmenistan. Meanwhile, China has become less dependent on arms imports, which decreased by 11 percent during 2012–16. While China was the largest importer globally by a wide margin in the early 2000s, it dropped to fourth place in 2012–16. However, China remains dependent on imports of key weapons systems and advanced components, including aerospace engines such as the Russian AI-31FN and RD-33 engines used on the J-10 and FC-1 fighters, respectively. In 2012–16, for example, aircraft engines accounted for 30 percent of China's arms imports, delivered from Russia (57 percent), Ukraine (16 percent), and France (15 percent).<sup>23</sup> These figures represent an ongoing shift in China's position on global arms markets, backed by increasing technological, organizational, and financial capabilities of China's military industrial complex as well as its growing global geostrategic interests.

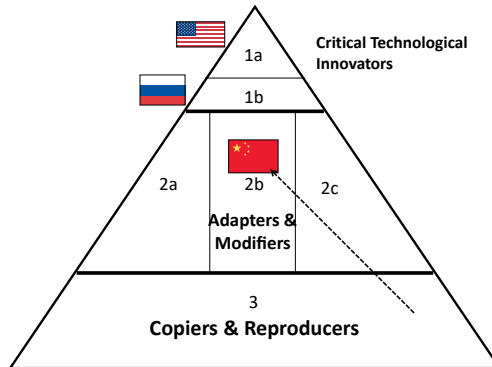
By narrowing the technological gaps with leading Russian and Western suppliers, China has been able to enter new markets with new-generation

military technologies, including Saudi Arabia, Morocco, Venezuela, Ecuador, Peru, Mexico, Nigeria, Kenya, Thailand, and Indonesia. In doing so, China's current arms export strategy has reflected varying "competitive" paths. In the developing countries of Latin America, Africa, and even Central Asia, China is trying to position itself as an alternative to Russian arms exports while counterbalancing the influence of Western powers. Chinese defense contractors compete on price while providing greater flexibility when negotiating the financial terms of arms contracts. However, Beijing's diplomatic relations with Moscow coupled with China's continuing dependence on imports of Russian advanced military technologies arguably precludes Chinese defense companies from fully contesting Russian arms export markets.

To project the impact of China's arms exports as well as its potential future paths and patterns, it is essential to project an analytical framework that may enable an assessment of China's defense innovation dynamics.<sup>24</sup> Indeed, the varying nature and character in the sources, drivers, paths, and patterns of military innovation indicate the need for a comparative approach in assessing China's innovation and arms exports trajectories. A policy-oriented framework, the Pyramid Model, is presented next to analyze the inputs, paths and patterns, processes, and outputs of China's military-technological innovation and prospective future trajectories. The Pyramid Model starts with the assumption that military innovation trajectories can be compared based on a hierarchy of a defense industrial base or "a sector or groups of industries that are dependent to some degree on defense spending and upon which the state is dependent on some degree of self-sufficiency in the production and the means of defense and war."<sup>25</sup> Keith Krause, a professor at the Graduate Institute of International and Development Studies in Geneva, broadly categorizes states' defense industries into three tiers: (1) critical technological innovators—states with a state-of-the-art technological edge in weapons R&D, (2) adapters and modifiers—characterized by a small but advanced defense industry, and (3) copiers and reproducers—low-technology arms producers.<sup>26</sup>

The first tier comprises those states with the capacity for across-the-board development and manufacture of advanced conventional weaponry. This tier consists of just a handful of countries: the United States and the four largest Western European arms producers (Britain, France, Germany, and Italy), as well as Russia. Given the US preponderance of defense-industrial capabilities, it might be more fitting to describe the United States as a Tier 1a country and the others as Tier 1b producer states.<sup>27</sup> The Soviet Union could have been classified as a Tier 1a producer state, but

given the more than 25 years of atrophy in its defense industrial base, Russia is struggling to remain in the first tier (missiles and combat aircraft remain its greatest strengths; even those systems, however, have their roots in Soviet R&D). The second tier consists of a rather small group of countries. Tier 2a comprises those industrialized countries with capabilities for advanced but nevertheless limited arms production (i.e., niche defense production), such as Australia, Canada, Israel, Norway, Japan, and Sweden. The second subgrouping (Tier 2b) consists of developing or newly industrialized countries containing modest (but in some cases, expanding) military-industrial complexes, such as Argentina, Brazil, Indonesia, Iran, South Africa, South Korea, Taiwan, and Turkey. Finally, there are Tier 2c producers such as India; these are developing industrial states with large, broad-based defense industries but still lacking sufficiently capable R&D and industrial capacities to develop and produce highly sophisticated conventional arms. At the bottom of the pyramid are various so-called Tier 3 states, possessing only very limited and generally low-tech arms production capabilities, such as the manufacture of small arms or the licensed assembly of foreign-designed system; countries in this group include Egypt, Mexico, and Nigeria (see figure below).



**China in the hierarchy of global arms industries.** (Developed by Richard Bitzinger and Michael Raska.)

In this framework, China has traditionally fallen into the category between a Tier 3 and Tier 2c arms producer.<sup>28</sup> However, progress in reforming the Chinese military-industrial complex over the past decade or so has been palpably evident in terms of the quality and capabilities of new weapons systems and of the increased tempo of defense development—indicating an ongoing shift toward Tier 2b and, in select areas, toward Tier 2a. At issue, therefore, is how well China's defense industry is performing vis-à-vis other arms-producing states. This comparative performance is

particularly critical to assess for two reasons. First, the “technological goal-posts” when it comes to weapons development are constantly moving; as certain nations—particularly the United States—advance the state of the art in defense technology, they create new metrics for defining what is meant by “advanced” military systems. Hence, the first question to ponder is whether China is keeping pace—or better yet, closing the gap—with the overall progress in military technological-industrial development. Second, a nation’s status in the global hierarchy of arms-producing states is not permanent; positioning is relative, depending on the ongoing performance of a nation’s defense industrial base. Consequently, countries can rise or fall along this scale. Russia is obviously on the fence as a future Tier 1 producer state, while it could be argued that South Korea could eventually become a Tier 2a state capable of producing a limited number of more advanced armaments. When using this model, therefore, the critical question to ponder is whether China is on the verge of becoming a Tier 1b arms producer.

### **Four Waves of Chinese Arms Exports**

In a historical perspective, the technological development of China’s defense industry has progressed gradually in four overlapping waves: (1) the Maoist era (1949–78), (2) Deng’s demilitarization era (1980s–1990s), (3) the reform era (1998–2012), and (4) Xi Jinping’s reform era 2.0 (2012–present).<sup>29</sup> Each era shaped the direction and character of Chinese arms exports. These four waves evolved through varying strategic drivers including ideological (1950s–60s), geopolitical (early 1970s), commercial (1980s), and competitive (2010s).<sup>30</sup>

In the early Maoist era, China’s defense industrial strategy and technological development reflected nearly total dependence on Soviet assistance. At that time, China’s defense sector was at the center of the economy, controlling heavy industrial sectors, and a principal engine driving China’s technological and industrial innovation development. The primary driver for arms exports, however, was ideological (i.e., China providing military assistance to Communist forces in French Indo-China (Vietnam) and to North Korea during the Korean War). From the late 1950s, China began to export its own weapons, based on acquired Soviet designs, to its allies—such as Albania, North Vietnam, and North Korea—as well as to newly independent African nations as part of its efforts to win greater influence among developing countries. Under Mao, China’s defense economy also had two parallel technological and industrial tracks: conventional and strategic weapons development. Innovation, however, diffused primarily in the

strategic sector with key programs such as Liangdan Yixing (2 Bombs and 1 Satellite program). With the Sino-Soviet split of the late 1960s, coupled with China's domestic political upheavals of the Great Leap Forward (1958–62) and the Cultural Revolution (1966–72), China's conventional base atrophied and innovation virtually disappeared.<sup>31</sup>

In the 1960s, China established close ties with Pakistan, which became the largest importer of Chinese weapons and remains so to this day. Establishing a strategic military-political alliance with a capitalist and pro-Western Pakistan marked the beginning of Beijing's Realpolitik strategy in the early 1970s, which prioritized pragmatic geopolitical and military considerations over ideology.<sup>32</sup> In particular, the principal assumption in Deng Xiaoping's Four Modernizations was that China no longer faced Cold War threats and should switch from militarization to economic development, liberalization, and "opening up" reforms. Therefore, China's defense industry should pursue concurrent development of dual-use technologies applicable in both civilian and military needs—principally under the Junmin Jiehe strategy: combining military and civilian activities, peacetime and wartime preparations prioritize military products and let the civilian sector support the military. Under Deng, China also launched the National High Technology Program ("863") in March 1986, aimed at developing seven strategic priority areas: laser technology, space, biotechnology, information technology, automation and manufacturing technology, energy, and advanced materials.

During the Iran-Iraq War (1980–88) China's arms exports were driven increasingly by commercial factors. In this period, China offered large quantities of affordable conventional weapons to both Iran and Iraq. After the breakup of the Soviet Union until 2000, however, China's arms exports fell sharply to about \$800 million a year.<sup>33</sup> Around that time, Chinese-made weapons—based on upgrades and copies of vintage Soviet designs of the mid-1960s—became truly obsolete, and China's defense industry lacked the ability to develop a new generation of weapons systems. Beijing also faced an arms import embargo from the West following the Tiananmen Square protests in 1989. The confluence of these factors forced China to become a net arms importer during much of the 1990s, primarily acquiring a range of modern Russian weapons and defense technologies while initiating defense industry reforms. Consequently, in the early 2000s, China's defense industry began to export advanced military technologies, either licensed or reversed-engineered from Russia or the Commonwealth of Independent States. Moreover, the industry was able to roll out a broad range of domestic new-generation systems. For example, from

2001 to 2005, China sold C-801 and C-802 anti-ship missiles, man-portable SAM systems, K-8 jet trainers, PLZ-45 self-propelled howitzers, and Al-Khalid tanks (Type 90) to Pakistan and Iran.<sup>34</sup>

Since 2005 onward, the product range, technological advancement, and relative quality of the catalog of Chinese-made arms offered for exports—particularly in areas such as aerospace—have made significant progress relative to the archaic offerings of the late 1990s. China introduced two fourth-generation fighters into mass production stage: the FC-1/JF-17 (developed jointly with Pakistan) and the J-10. It increased its presence in international aerospace and defense markets, promoting its new combat trainers (FTC-2000, L-15, K-8), fifth-generation fighter (J-31), missile systems (anti-ship, anti-tank, and man-portable), SAMs (HQ-9), radars (YLC-8B, SLC-2E), transport aircraft (MA60, Y-20), helicopters (Z-9G, Z-10, Z-11, Z-15, Z-19E); UAVs (Pterodactyl WJ-1, CH-4), new versions of the Type 90 tank (VT-3, VT-4, VT-5), a new generation of light armored vehicles (VN-4), self-propelled and towed artillery (PLZ45, PLZ52), multiple rocket launchers (A-100), trucks (CS/VN3), ships (Type 053, 054A, 056), and submarines (S26T/Type 039A).<sup>35</sup>

### **China as an Arms Supplier in the Twenty-First Century**

China has regularly been listed as being among the world's top five arms exporters for the past 20 years, along with such traditional leading suppliers as the United States, Russia, France, and the United Kingdom. The best data we have regarding China's place in the international arms marketplace comes mainly from two sources: SIPRI and the US Congressional Research Service (CRS). SIPRI data for 2014–18 shows China to be the world's fourth-largest arms exporter, with 5.2 percent of the global market. This performance places it behind the United States (the number one arms exporter, with 36 percent of the international arms market) and Russia (with 21 percent) and roughly even with France (6.8 percent), Germany (6.4 percent), and the United Kingdom (4.2 percent).<sup>36</sup>

Congressional Research Service data covers a slightly different time frame but tells a similar story. According to the CRS, China was fifth in terms of *arms deliveries* for the period 2012–15 (valued at US \$9.6 billion); this was good for about 5 percent of the overall international arms market. In 2015 alone, it was fourth in terms of arms deliveries, worth US \$2.9 billion. In comparison, the United States accounted for nearly one-third of total international arms deliveries for the period 2012–15, while Russia was second at nearly 20 percent.<sup>37</sup> In terms of *arms sales agreements*, Chinese overseas arms sales have averaged more than \$3.6 billion a year for

the period 2008–15; this compares quite favorably with the country's experiences as an arms exporter during the 1990s, when Beijing averaged less than \$1 billion annually in arms sales. In 2015 alone, China concluded \$6 billion worth of arms sales.<sup>38</sup>

Nearly all of China's arms transfers are to developing countries, and in this arena the Chinese defense industry has emerged as a formidable competitor to Western and Russian arms exporters. China's main arms markets are in Asia and the Middle East, and about three-quarters of its weapons exports go to countries in these regions. In addition, China has become a leading arms supplier to Africa; in 2012–15, in fact, China was the single largest supplier to Africa, capturing nearly one-third of the continent's overall arms market, surpassing exports from Europe, Russia, and the United States.<sup>39</sup> Major customers for Chinese arms include Algeria, Bangladesh, Egypt, Iran, Myanmar, Nigeria, Pakistan, Sri Lanka, Sudan, Tanzania Zimbabwe, and Zambia. More recently, Venezuela has become a significant customer for Chinese arms, giving China a toehold in Latin America, with deliveries of VN-4 "Rhinoceros" carriers, K-8 trainer aircraft, VN-16 light tanks, and VN-18 infantry fighting vehicles.<sup>40</sup> Many of China's arms deals have been done at "friendship prices" or in Beijing's terms "flexible payment methods," that is, selling arms at a discount or on credit. Such agreements have been made either for political purposes (i.e., cementing alliances or promoting cordial relations) or, increasingly, to secure links with oil- and mineral-rich nations, such as Venezuela, Nigeria, Sudan, and Zimbabwe. For example, according to China Military Online—the PLA's official news website—China agreed to use oil for partial payment in the above-mentioned China-Venezuela arms deal. Also, its exports of armored vehicles to Thailand have been financed with dried foods, and the Chinese FD-2000 long-range air defense missile systems exported to Uzbekistan and Turkmenistan have been exchanged for natural gas.<sup>41</sup>

### ***Recent Chinese Arms Export Activities***

Leading Chinese arms exports currently include the following:

- *Type 039A Yuan-class submarine*: This attack submarine, manufactured by the China Shipbuilding Industry Corp. (CSIC), features a modern teardrop hull and carries both torpedoes and ASCMs, and it may even be equipped with an as-yet-unidentified system for air-independent propulsion. China recently sold eight Yuan-class submarines to Pakistan (export version designated as S20) and three to Thailand (S26T).<sup>42</sup>



- *Unmanned aerial systems and armed drones:* China has quite recently become one of the world's largest manufacturers of various UAVs, ranging from the very small, handheld types all the way up to very large high-altitude, long-endurance (HALE) drones. In particular, China has so far exported at least two types of *armed* drones, the Caihong and the Wing Loong (also called the Pterodactyl) series. The Wing Loong has been sold to Egypt, the United Arab Emirates, and Saudi Arabia.<sup>43</sup> A larger version, the Wing Loong II, is also available. The Caihong (Rainbow) has been sold to Nigeria, Egypt, and Iraq. It has already been used in military operations in Africa against Boko Haram militants, while Iraq has employed the Caihong in attacks on ISIS targets.<sup>44</sup>
- *JF-17 Thunder fighter jet:* The JF-17, also known as the FC-1, is a lightweight multirole combat aircraft similar in design to the US F-20 Tigershark. The JF-17 was co-developed with Pakistan, currently producing the fighter for its air force; estimates are that Islamabad could buy up to 250 of the aircraft. The aircraft is being specifically marketed to developing countries that need to replace aging MiG-21, F-7, or F-5 fighters.<sup>45</sup>
- *C-801/C-802 anti-ship cruise missile (ASCM):* These missiles, also known as the YJ-8 and YJ-82 (YJ stands for "Yingji" or "Eagle Strike"), respectively, are similar to the very effective French Exocet (the C-802 version being equipped with a solid rocket booster for extended range). These ASCMs can be launched from ships, land, or aircraft. Recent customers for these missiles include Algeria, Bangladesh, Indonesia, Iran, Myanmar, Pakistan, and Thailand.<sup>46</sup>
- *K-8 trainer jet:* China has had great success in selling the K-8 lightweight trainer/attack jets, exporting over 300 of these planes since 2000. Its biggest client has been Egypt, which bought 120 K-8s, most of which were assembled locally from kits; Myanmar plans to license/assemble up to 50 of these aircraft. Other customers include Bolivia, Ghana, Namibia, Pakistan, Sri Lanka, Sudan, Tanzania, Venezuela, Zambia, and Zimbabwe.<sup>47</sup>
- *F-7MG fighter jet:* This aircraft is the export version of the PLA Air Force's F-7E, itself an upgraded adaptation of the MiG-21. The F-7MG features a larger wing and, reportedly, a British radar. China has sold more than a hundred of these fighters to Bangladesh, Namibia, Nigeria, Pakistan, Sri Lanka, and Tanzania, according to the SIPRI Arms Transfers database, since the mid-1990s.<sup>48</sup>

- *FD-2000 surface-to-air missile system*: It is the export version of the HQ-9, a primary long-range SAM system of the PLA on land and at sea, analogous in its capabilities to the Russian S-300. It has gained considerable attention since “Turkey selected the FD-2000 in 2015 before US pressure forced Ankara to restart the tender process, resulting in the selection of Russia’s S-400. China, however, exported the FD-2000 to Uzbekistan and Turkmenistan, while Pakistan is reportedly considering its acquisition to counter India’s recent contract with Russia for S-400.”<sup>49</sup>
- *VT4 (MBT-3000) main battle tank*: The VT4 is a 52-ton MBT designed and manufactured by the China North Industries Corporation (NORINCO) specifically for the export market. It integrates the latest PLA technologies within the Type 99A MBT. In 2016–17, China delivered an initial batch of 28 VT4s to Thailand, while Pakistan selected the VT4 in 2018 to modernize its MBT fleet.<sup>50</sup>
- *WZ-551 armored personnel carrier*: Although not a particularly high-tech system, the WZ-551 is notable for being sold widely around the world, including to countries like Argentina, Gabon, Kenya, Kuwait, Nepal, Oman, Sri Lanka, Sudan, and Tanzania.<sup>51</sup>

It is also worth noting that China has sold several types of small and medium-sized transport aircraft, mostly to African states. These include the Y-12 (to Kenya, Nepal, Uganda, and Zambia) and the MA-60 (to Ghana, Nepal, and Zambia).<sup>52</sup> Other military items with considerable export potential include two locally manufactured combat aircraft, the J-10 and the J-31 fighter jets. The J-10 is roughly equivalent in capability to the US F-16C. Development of the J-10 began in the mid-1980s, and it entered service with the People’s Liberation Army Air Force (PLAAF) in the early 2000s. The J-31 is a putative “fifth-generation” combat aircraft currently under development, closely resembling the US-designed F-35 Joint Strike Fighter. It first flew in October 2012. In fact, there has been considerable speculation that the Chinese might try to flood the global arms market with the J-10 and the J-31. Both these combat aircraft could potentially be stiff competition for Western or Russian fighter jets—especially if offered at cut-rate prices—the J-10 competing against smaller, single-engine aircraft such as the Swedish Gripen and the J-31 going up against the Typhoon, Rafale, or the F-35. Pakistan has reportedly agreed to buy 36 J-10s, and Iran is rumored to be interested in the fighter as well.<sup>53</sup> Other potentially marketable products include the YJ-7/C-701 short-range ASCM (already sold to Iran and, reportedly, Hezbollah<sup>54</sup>),

the FN-6 man-portable SAM (exported to Malaysia and Peru, among other countries), and the KS-1A SAM missile (sold to Myanmar and Thailand).<sup>55</sup>

### ***Chinese Armed Drones: A Special Case Study***

As noted previously, China has quite recently but also quite significantly become a key exporter of armed drones (also referred to as unmanned combat aerial vehicles or UCAVs).<sup>56</sup> This is troubling because not only are they a potentially lucrative segment of the arms business that is likely to grow appreciably over the coming decades—and therefore challenging US sales—but armed drones are also a mounting proliferation concern, seeing as they are an extremely effective offensive weapon.

Only a handful of countries presently manufactures dedicated armed drones. China is one of them. Moreover, China is one of the few countries, other than the United States and Israel, perhaps, whose UCAVs have actually been used in combat. In particular, the Iraqi military recently used a Chinese-built CH-4B Caihong (Rainbow) drone to attack an ISIS target—in this case, with a laser-guided missile. It was, Iraq's first-ever drone strike.<sup>57</sup> In fact, largely unnoticed by most observers, China has become a leader in the global sale of armed drones—especially medium-altitude, long-endurance UAVs. It has so far exported two armed drone series, the Caihong and the Wing Loong, manufactured by China Aerospace Science and Technology Corporation (CASC) and Chengdu Aircraft Industry Group (CAIG), respectively.<sup>58</sup> Both bear a striking resemblance to two existing US UCAVs, the MQ-1B Predator and the MQ-9 Reaper. The Wing Loong, designed and built by CAIG, is roughly the same size as the Predator, about 29 feet long and with a wingspan of 45 feet. It carries a much smaller payload, however, about 220 pounds, compared to the Predator's 1,100 pounds. However, the Wing Loong costs about a million dollars per unit, or only one-fourth that of a Predator drone. It has been sold to Egypt, the United Arab Emirates, Saudi Arabia, and, most recently, to Serbia.<sup>59</sup>

The Caihong drone was developed by the CASC, and it is perhaps more disconcerting as a weapons platform than the Wing Loong I and II series. The original CH-3 version, which had been sold to Nigeria, appears to be relatively ineffective as a UCAV; at least one crashed in Nigeria in 2015, ostensibly during operations against the Boko Haram militants.<sup>60</sup> The CH-4, however, is more or less a clone of the MQ-9 Reaper and much more capable. It carries a relatively small payload, about 350 kilograms, but larger, improved versions are on the way. In addition to Iraq, the CH-4

has been sold to Egypt and Saudi Arabia.<sup>61</sup> More importantly, there is a new, larger version of the Caihong drone, the CH-5, being readied for market. The CH-5 has a wingspan of 20 meters (66 feet) and a takeoff weight of about 3 tons. It can carry a maximum payload of around 900 kilograms—about two and a half times more than previous UCAVs in the CASC Rainbow series.<sup>62</sup> Finally, China is reportedly developing a purpose-built, low-observable drone, dubbed “Lijian” (Sharp Sword). Although still a proof-of-concept prototype, the Lijian first flew in 2013 and could be the precursor to a family of Chinese stealth UCAVs.<sup>63</sup>

More nations are acquiring armed drones, and more are building them; consequently, UCAVs are poised to become a significant proliferation concern. The United States is a major drone-producing country, but it has considerable controls over the export of these systems. China, on the other hand, has relatively few scruples when it comes to what and to whom it sells its military wares. Armed drones are one of the few areas of the global arms market where China could carve out quite a lucrative niche for itself, to the potential detriment of the US and its allies. Finally, a large chunk of Chinese arms exports includes small arms and ancillary equipment, such as trucks, uniforms, and field equipment. Particularly when it comes to sub-Saharan Africa, China has become a leading supplier of assault rifles, ammunition, mortars, and the like. In one case, UN inspectors found that high-explosive incendiary cartridges, ostensibly Chinese in origin, were used in Darfur in the early 2010s. At the same time, Beijing has stymied UN efforts to investigate arms flows into Africa.<sup>64</sup>

In this context, China will continue to be an important arms exporter, albeit with limitations. It is unlikely, for instance, that Chinese weaponry will constitute much of a threat to European arms manufacturers. Many of Europe’s key customers will probably remain reluctant to buy Chinese armaments for a variety of reasons. They may have acrimonious or even hostile relations with China and would not wish to employ or depend on Chinese armaments. Conversely, countries may purposely acquire European armaments to strengthen political-military relations with Europe, which they may value more than similar ties with China.

Arms buyers may also prefer European (or other Western or Russian) armaments because they view these weapons to be more reliable and capable than their Chinese counterparts. The J-10, for example, may be a very good aircraft, but since its performance and reliability cannot be independently confirmed, many countries may not want to take the chance. Moreover, countries do not necessarily buy the cheapest weapon systems available—other attributes often count more, such as military effective-

ness and after-sales support. This is especially so when it comes to military products; many countries—particularly the best customers on the global arms markets—given the choice, will still pay a premium price to get a premium product.

That said, there are a few areas where more advanced Chinese weapons systems could challenge European arms exporters. These include diesel-electric submarines (potentially affecting French, German, and Swedish submarine producers); anti-ship, surface-to-air, and anti-tank tactical missile systems (potentially affecting companies like MBDA, Saab Dynamics, and Thales); and (increasingly) UAVs and armed drones (such as the Dassault nEUROn or the Airbus Barracuda)—all segments where China already has demonstrated expertise and has scored prior export sales. Potential *future* areas of competition could include fighter aircraft, defense electronics (such as radar systems), and surface combatants. In this regard—and including small arms—Chinese arms sales successes vis-à-vis their European competitors would probably lie mostly at the low end (i.e., poorer countries for whom money is definitely an issue).

### **Advancing Geostrategic Interests**

Chinese overseas arms transfers have even begun to put a dent into Russian arms export efforts. China competes directly with Russia for arms markets in the developing world, particularly Africa, South and Southeast Asia, and Latin America. Beijing has captured sales in countries that were major customers for the Soviet Union/Russia, such as Algeria (frigates, ASCMs, artillery systems), Cambodia (helicopters, man-portable SAMs), Egypt (combat aircraft, UAVs), Ethiopia (armored personnel carriers, SAMs), Iran (ASCMs, SAMs), Iraq (UAVs), and Venezuela (combat aircraft, multiple rocket launchers, SAMs). China has also scored some minor deals with Russian client states such as Kazakhstan, Syria, and Turkmenistan.<sup>65</sup> However, Russia's most important arms buyers remain unassailable by Chinese arms industries. Countries like India (that accounted for 27 percent of all Russian overseas arms deliveries during the period 2014–18), South Korea, and Vietnam are in inimical relationships with Beijing and thus would probably never buy arms from China (or would not purchase them for political reasons). Ironically, China continues to be one of Russia's biggest arms buyers (and the sixth-largest arms *importer* overall) for 2014–18.<sup>66</sup> It accounted for 14 percent of Russian arms transfers during this period.<sup>67</sup>

For the most part, China's arms industry does not seriously threaten US arms exports, at least not in terms of quantity. Again, according to SIPRI

data, China garnered only 5.2 percent of the total global arms market—only good enough to take the number five spot but still well behind the United States. Moreover, from 2014 to 2018, the bulk of China's weapons shipments—nearly two-thirds (64 percent)—went to just three countries, namely Pakistan, Bangladesh, and Algeria.<sup>68</sup>

Constraining or limiting the global transfer of conventional armaments is also a challenge for Beijing, especially when it might affect its use of arms sales as a producer of profits or a promoter of strategic influence. China does have a formalized, legal, and regulatory framework for approving and overseeing arms transfers, that is, "The Regulations of the People's Republic of China on the Administration of Arms Export" (established in 1997 and amended in 2002). According to a publication put out by Saferworld, "This represented a shift from an administratively based system in the form of executive decrees, to a system based on law and regulations that is more thoroughly codified and transparent."<sup>69</sup> In this regard, the regulations set out the three principles guiding decision-making on Chinese arms transfers: self-defense; peace, security, and stability; and noninterference. Moreover, China has also had a declaratory policy of not transferring weapons to non-state actors.<sup>70</sup> Nevertheless, Beijing does not seem to strenuously advocate for arms control. China, for example, was one of 22 countries to abstain on the April 2013 UN General Assembly resolution to adopt the Arms Trade Treaty. Moreover, it has in the past sold arms to pariah states (e.g., Iran or North Korea) even after it said that it would not, and it has opposed international efforts to impose sanctions and arms embargoes. It also makes little effort to control so-called third-party re-exports of Chinese-made weaponry. Compounding all this is a decided lack of transparency in the Chinese arms export approval process.<sup>71</sup> In 2019, the National People's Congress Standing Committee began to draft a new law that would impose tighter controls on China's arms and nuclear technology sales while consolidating the existing fragmented export controls. Under the new law, for example, arms exporters would have to establish an internal compliance review system, while government agencies would also have to assess buyers and take corresponding risk control measures.<sup>72</sup> However, conforming to this new set of regulations would also require increased transparency in the secretive world of Chinese weapons diplomacy, which will likely face considerable internal challenges.

In the long term, China is likely aiming to leverage arms exports as an instrument of its foreign policy to project power, presence, and influence in areas vital to China's interests, such as in South and Southeast Asia.

Beijing is starting to position state-owned defense enterprises to support the Chinese government's BRI strategy to deepen economic links with developing regions and, in doing so, create new pathways for strategic dependencies. Under the guidance of China's State Administration for Science, Technology, and Industry for National Defense (SASTIND), for example, in May 2019, China State Shipbuilding Corporation (CSSC) and China Poly Group Corporation signed a long-term agreement to collaborate on naval export opportunities integrating military technologies and capabilities in international markets related to the BRI.<sup>73</sup> However, the assertion that Chinese arms sales are an instrument of foreign policy is still open to debate. A recent IISS study notes that there has been no increase in Chinese arms deliveries to core BRI partner countries since 2013: "out of the 74 countries that are directly linked to BRI projects, only 23 of them—31 percent—have received Chinese major weapon systems since 2013."<sup>74</sup> In this view, Chinese arms sales have been largely transactional rather than strategic.

The contending view is that notwithstanding the majority of China's arms exports between 2012 and 2016 going to South Asian countries such as Pakistan (35 percent), Bangladesh (18 percent), and Myanmar (10 percent),<sup>75</sup> these countries provide critical alternative routes of energy supplies from the Middle East to China. Both Pakistan and China also have overlapping territorial claims with India. At the same time, there are indicators that China is trying to counterbalance the US—China's recent major arms exports contracts with Thailand (S26T submarines) and military assistance to the Philippines could be viewed as an attempt to mitigate the inclusion of the United States. In a reverse mode, these countries may seek Chinese defense contracts to solidify security and economic ties with China. Regardless of the range of contending debates about China's political aims and strategic trajectories, the nature of the emerging strategic competition is whether China will have the requisite capabilities to project power in Asia and beyond on par with the United States, and how the United States and its key allies in unison with other major powers will respond to such changes.<sup>76</sup> Consequently, China arguably aims to shape the direction and character of the arms competition—not only through its own military-technological development but also by imposing strategic choices on others to reshape the future balance of power in different geographic areas.

## **Conclusion**

Despite recent glowing sales figures, China's current position in the global arms marketplace remains tenuous. First, it remains a niche player in the global arms market because it sells most of its weapons to very few countries. Moreover, according to SIPRI, while China sold major arms to 53 countries during 2014–18, 39 of them each accounted for less than one percent of total Chinese arms exports.<sup>77</sup> In fact, China faces a continual challenge of remaining viable in the highly competitive business of international arms transfers. China continues to struggle with remaining technologically competitive with the West, particularly when it comes to developing and manufacturing more advanced types of weaponry—such as supersonic combat aircraft, precision-guided weapons, airborne early warning aircraft, and long-range air defense systems. Armed drones, anti-ship cruise missiles, and submarines aside, China can for the most part still offer only a handful of advanced weapons systems that are competitive in the global arms market. Beijing has won very few orders for its most advanced fighter jets, particularly the JF-17 and the J-10. The only sizable sale of the JF-17 has been to Pakistan—and only because Pakistan is producing the plane jointly with China (in addition, Myanmar has ordered 16 JF-17s and Nigeria three); not even the PLAAF has acquired the JF-17, in fact. Also, as of January 2020, no export order for the J-10 (to Pakistan or any other air force) has yet been consummated.

Furthermore, even when countries have purchased Chinese weapons systems, they often throw out Chinese components and replace them with Western systems. This is because China's defense industry is still very weak when it comes to key technologies such as jet engines and electronics. For instance, Algeria acquired corvettes from China but subsequently outfitted them with Western-made radar, fire-control, and communications gear. Pakistani JF-17 jets use a Russian engine, while Thailand turned to Saab to upgrade its Chinese-built frigates.<sup>78</sup>

A second challenge for China is to continue expanding its customer base. For the most part, Beijing has mainly sold military equipment to countries either too poor to buy Western or Russian armaments (such as sub-Saharan African states and Myanmar) or that have been subjected to arms embargoes (such as Iran and Venezuela). Few wealthy, big-spending arms importers (such as the oil-rich Gulf states) have ever been interested in Chinese arms, other than a handful of low-end items<sup>79</sup> (notable exceptions: both the United Arab Emirates and Saudi Arabia have recently acquired armed drones from China). Iran was a major consumer of Chinese arms, but it has not placed a new order with Beijing in several




years. Similarly, China has found relatively few takers for its arms in Latin America, Eastern Europe, or Central Asia. A \$3.4 billion deal to sell air defense missiles to Turkey collapsed under pressure from Ankara's NATO allies.<sup>80</sup>

China may hold the number three slot in the global arms trade, but it is still far behind the United States, with 33 percent of the global market, and Russia, with 25 percent. In fact, China is only slightly ahead of France (5.6 percent), Germany (4.7 percent), and the United Kingdom (4.5 percent). Moreover, China's position in the global hierarchy of arms exporters has been inconsistent. According to SIPRI, during the period 2006 to 2010, China won just 3.7 percent of the total arms market, placing it sixth in overall weapons exports. Nevertheless, China's cumulative political, economic, and military rise is reshaping global as well as regional geopolitics, including strategic alliances and balance of power in East Asia in ways that are inherently detrimental to established great powers (i.e., US interests and its regional strategic partners and allies). While the US continues to maintain superior military-technological advantages and regional presence, its ability to underwrite stability in the Asia-Pacific region is increasingly challenged by China.<sup>81</sup> The resulting Sino-US strategic competition, reflected for example in the emerging US Third Offset Strategy, in turn compels smaller and medium-sized states in Southeast Asia to accelerate military modernization, particularly naval and air forces, to keep vital sea-lanes open, conduct intelligence missions, and perhaps most importantly, provide strategic options to respond in the Sino-US competition.

These trends exacerbate regional "arms competition," characterized by incremental, often near-continuous, improvements of existing capabilities. In a mix of cooperative and competitive pressures, it also includes continued purchases of advanced weapon platforms—including the introduction of new types of arms and, therefore, unprecedented military capabilities.<sup>82</sup> China has a growing capability to shape the direction and character of the arms competition—not only through its military-technological development and diffusion of arms exports, but more importantly, through its strategic choices that influence the contours of strategic alliances and balance of power in different geographic areas. Accordingly, the ongoing struggle for dominance by the region's two major powers (China and Japan); the future of the Korean Peninsula; intraregional competition in territorial disputes in the East China Sea and South China Sea; and, perhaps most importantly, the contours of long-term regional strategic competition and rivalry between China and the United States will be

inherently shaped by attendant consequences of China's defense industrial strategies aligned with Beijing's geopolitical and economic aspirations.

In summary, Chinese arms exports may have had their beginnings in mostly transactional economic rationales—such as profits and support for the domestic arms industry. However, increasingly overseas arms sales may be seen as a tool to advance Beijing's strategic interests.

As such, they will also increasingly figure in the growing strategic competition with the United States. Beijing's evolving strategy of indigenous innovation in a broader context of civil-military integration constitutes a pathway for China's long-term strategic competition.<sup>83</sup> In doing so, China continues to seek niche technological developments that could potentially revolutionize the PLA's military operations by providing a credible asymmetric edge in regional flashpoints in East Asia (e.g., anti-ship and anti-satellite ballistic missiles, hypersonic cruise missiles, and systems converging cyber and space capabilities). Such technology has been evident in the gradual, dual-track military modernization trajectory of the PLA, characterized by upgrading its existing arsenal of legacy weapons systems and platforms while experimenting with the next generation of design concepts. Notwithstanding these advanced military-technological goalposts, China's strategy will be increasingly influenced by its ability to align its political and strategic goals with corresponding military capabilities.<sup>84</sup> This includes China's ability to alter strategic alliances and balance of power through international arms exports, technology transfers, and defense cooperation. 

### Michael Raska

Michael Raska is an assistant professor and coordinator of the Military Transformations Program at the S. Rajaratnam School of International Studies, Nanyang Technological University in Singapore. His research interests focus on East Asian security and defense issues, including theoretical and policy-oriented aspects of military innovation, force modernization, information conflicts, and cyberwarfare. He is the author of *Military Innovation and Small States: Creating a Reverse Asymmetry* (Routledge, 2016) and co-editor of *Security, Strategy, and Military Change in the 21st Century: Cross-Regional Perspectives* (Routledge, 2015).

### Richard A. Bitzinger

Richard A. Bitzinger is a senior visiting fellow at the S. Rajaratnam School of International Studies in Singapore. He has written extensively on Asian defense and military issues. His most recent books are *Arming Asia: Technonationalism and Its Impact on Local Defense Industries* (Routledge, 2017) and *Reshaping the Chinese Military: The PLA's Roles and Missions in the Xi Jinping Era* (Routledge, 2018).

### Notes

1. Jeffrey Lin and P. W. Singer, "The Dragon Muscles In: Growing Number of Victories in Chinese Arms Exports," *Popular Science*, 9 June 2016, <http://www.popsoci.com/>.

2. Nick Childs and Tom Waldwyn, "China's Naval Shipbuilding: Delivering on Its Ambition in a Big Way," *IISS Military Balance Blog*, 1 May 2018, <https://www.iiss.org/blogs/>.
3. Richard Bitzinger and Michael Raska, "Capacity for Innovation: Technological Drivers of China's Future Military Modernization," in *The Chinese People's Liberation Army in 2025*, eds. Roy Kamphausen and David Lai (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015), 144, <https://apps.dtic.mil/>.
4. Michael Mazarr et al., *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives* (Santa Monica, CA: RAND Corporation, 2018), <https://www.rand.org/>.
5. You Ji, "China's Emerging National Strategy," *China Brief*, 24 November 2004.
6. Tai Ming Cheung, "Dragon on the Horizon: China's Defense Industrial Renaissance," *Journal of Strategic Studies* 32, no. 1 (February 2009): 30–31.
7. Michael Raska, "Scientific Innovation and China's Military Modernization," *The Diplomat*, 3 September 2013, <https://thediplomat.com/>.
8. DOD Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013), <https://defenseinnovationmarketplace.dtic.mil/>.
9. Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies* 34, no. 3 (2011): 343–44; and Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, 1 June 2015, <https://www.csis.org/>.
10. Cheung, 343–44.
11. Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, eds. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 66.
12. Michael S. Chase et al., *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (PLA)* (Santa Monica, CA: RAND Corporation, 2015), 69, <https://www.rand.org/>.
13. You Ji, *China's Military Transformation: Politics and War Preparation* (Cambridge: Polity Press, 2016).
14. Cheung, "Chinese Defense Economy's Long March"; and Kennedy, "Made in China 2025."
15. Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004*, white paper (Beijing: State Council Information Office), 27 December 2004, <http://www.china.org.cn/>; and Eric Hagt, "Emerging Grand Strategy for China's Defense Industry Reform," in *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military*, eds. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: US Army War College, 2010), 481–84, <https://publications.armywarcollege.edu/>.
16. Tai Ming Cheung, ed., *Forging China's Military Might: A New Framework for Assessing Innovation* (Baltimore: Johns Hopkins University Press, 2013).
17. President Xi has stated that "military-civilian cooperation, as a national strategy, is crucial to national security and the bigger picture of development." Xinhua, "Xi Urges Greater Military-Civilian Cooperation for Strong Army," 20 October 2016, Ecns.cn, <http://www.ecns.cn/>.

18. Xinhua, "China Targets Better Integrated Military, Civilian Development," *China Military*, 22 July 2016, <http://english.chinamil.com.cn/>.
19. Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the "Going Out" of China's Defense Industry* (Washington, DC: Pointe Bello, 2016), <https://toinformistoinfluence.files.wordpress.com/>.
20. Zhao Lei, "Civil-Military Integration Will Deepen," *China Daily*, 3 March 2018, <http://www.chinadaily.com.cn/>; and Minnie Chan, "Chinese Military Sets Up Hi-Tech Weapons Research Agency Modelled on US Body," *South China Morning Post*, 25 July 2017, <https://www.scmp.com/>.
21. Tai Ming Cheung et al., *Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development; A Report Prepared for the U.S.-China Economic and Security Review Commission* (San Diego, CA: University of California, Institute on Global Conflict and Cooperation), 2016, 120, <https://www.uscc.gov/>.
22. Information Office of the State Council of the People's Republic of China, *China's Military Strategy*, white paper (Beijing: Ministry of National Defense, 26 May 2015), pt. 4, <http://eng.mod.gov.cn/>.
23. Aude Fleurant et al., *Trends in International Arms Transfers, 2016*, SIPRI Fact Sheet (Solna, Sweden: Stockholm International Peace Research Institute [SIPRI], February 2017), <https://www.sipri.org/>.
24. Tai Ming Cheung, Thomas G. Mahnken, and Andrew L. Ross, "Frameworks for Analyzing Chinese Defense and Military Innovation," *SITC Policy Brief*, no. 27 (September 2011), <https://escholarship.org/>.
25. John Paul Dunne, "The Defense Industrial Base," in *Handbook of Defense Economics*, vol. 1, Keith Hartley and Todd Sandler, eds. (Amsterdam: Elsevier, 1994), 399–430, [https://doi.org/10.1016/S1574-0013\(05\)80016-X](https://doi.org/10.1016/S1574-0013(05)80016-X).
26. Keith Krause, *Arms and the State: Patterns of Military Production and Trade* (Cambridge: Cambridge University Press, 1992).
27. Bitzinger et al., "Locating China's Place in Global Defense Economy," in Cheung, *Forging China's Military Might*.
28. Bitzinger et al.
29. Tai Ming Cheung, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Ithaca, NY: Cornell University Press, 2009).
30. Mikhail Barabanov, Vasily Kashin, and Konstantin Makienko, *Shooting Star: China's Military Machine in the 21st Century* (Minneapolis: East View Press, 2012), 77.
31. Cheung, *Fortifying China*.
32. Barabanov, Kashin, and Makienko, *Shooting Star*, 78.
33. Barabanov, Kashin, and Makienko, 78.
34. Barabanov, Kashin, and Makienko, 80.
35. Michael Raska, "China: Strategy and Challenges," in *Defence Industries in Russia and China: Players and Strategies*, eds. Richard A. Bitzinger and Nicu Pepescu, ISSUE Report no. 38 (Paris: EU Institute for Security Studies, 2017), <https://www.iss.europa.eu/>.
36. Pieter D. Wezeman et al., *Trends in International Arms Transfers, 2018*, SIPRI Fact Sheet (Solna, Sweden: Stockholm International Peace Research Institute [SIPRI], March 2019), table 1, 2, <https://www.sipri.org/>.
37. Catherine A. Theohary, *Conventional Arms Transfers to Developing Nations, 2008–2015* (Washington, DC: Congressional Research Service, 19 December 2016), 27, <https://fas.org/>.

38. Theohary, 29.
39. Theohary, 29.
40. Kristin Huang, "Venezuela Sends in China-Built 'Rhinos' Vehicles to Quell Anti-Government Protests," *South China Morning Post*, 3 May 2019, <https://www.scmp.com/>.
41. Ma Yao, "How China Becomes Third-Largest Supplier of Weapons Worldwide?," *China Military Online*, 27 February 2018, <http://english.chinamil.com.cn/>.
42. Global Security, "Type 039A Yuan-Class—Exports," *Global Security*, 1 January 2019, <https://www.globalsecurity.org/>.
43. Sharon Weinberger, "China Has Already Won the Drone Wars," *Foreign Policy*, 10 May 2018, <https://foreignpolicy.com/>.
44. Patrick Boehler and Gerry Doyle, "Use by Iraqi Military May Be a Boon for China-Made Drones," *The New York Times*, 17 December 2015, <https://www.nytimes.com/>.
45. "Myanmar First Country to Purchase JF-17 Thunder from Pakistan," *Dunya News*, 9 July 2015; and Jeremy Binnie, "Nigeria Waiting for US to Approve Super Tucano Sale," *Jane's Defence Weekly*, 7 June 2016, <https://defence.pk/>.
46. Stockholm International Peace Research Institute (SIPRI), SIPRI Arms Transfers Database, 11 March 2019, <https://www.sipri.org/>.
47. SIPRI Arms Transfers Database.
48. SIPRI Arms Transfers Database.
49. Joshua Kucera, "Has China Made Its First Big Military Sale in Central Asia?," *Eurasianet*, 6 February 2015, <https://eurasianet.org/>.
50. Mike Yeo, "Thailand to Buy More Chinese Tanks, Reportedly for \$58M," *Defense News*, 4 April 2017, <https://www.defensenews.com/>.
51. SIPRI Arms Transfers Database.
52. SIPRI Arms Transfers Database.
53. Siva Govindasamy, "Pakistan Signs Deal for Chinese J-10 Fighters," *FlightGlobal*, 13 November 2009, <https://www.flightglobal.com/>; and Zachary Keck, "Get Ready, Israel: China to Sell Iran Advanced Fighter Jets?," *The Buzz* (blog), *The National Interest*, 5 August 2015, <https://nationalinterest.org/>.
54. SIPRI Arms Transfers Database.
55. SIPRI Arms Transfers Database.
56. Benjamin David Baker, "Drone Wars: China and US Compete on the Global UAV Market," *The Diplomat*, 25 October 2015, <https://thediplomat.com/>.
57. "Iraq Shows Off Airstrike by New Chinese-Made Combat Drone (VIDEO)," *RT News*, 16 October 2015, <https://www.rt.com/news/>.
58. Greg Waldron, "China Finds Its UAV Export Sweet Spot," *FlightGlobal*, 14 June 2019, <https://www.flightglobal.com/>.
59. Franz-Stefan Gady, "China, Pakistan to Co-Produce 48 Strike-Capable Wing Loong II Drones," *The Diplomat*, 9 October 2018, <https://thediplomat.com/>.
60. Jeffrey Lin and P. W. Singer, "Did an Armed Chinese-Made Drone Just Crash in Nigeria?" *Popular Science*, 28 January 2015, <https://www.popsoci.com/>.
61. Minnie Chan, "Chinese Drone Factory in Saudi Arabia First in Middle East," *South China Morning Post*, 26 March 2017, <https://www.scmp.com/>.
62. China Power Project, "Is China at the Forefront of Drone Technology?," Center for Strategic and International Studies, 29 May 2018, <https://chinapower.csis.org/>.

63. Jeffrey Lin and P. W. Singer, "Meet China's Sharp Sword, a Stealth Drone That Can Likely Carry 2 Tons of Bombs," *Popular Science*, 18 January 2017, <https://www.popsci.com/>.
64. Colum Lynch, "China's Arms Exports Flooding Sub-Saharan Africa," *The Washington Post*, 25 August 2012, <https://www.washingtonpost.com/>.
65. SIPRI Arms Transfers Database.
66. SIPRI Arms Transfers Database.
67. Wezeman et al., *Trends in International Arms Transfers*, 2018, table 2, 6.
68. Wezeman et al., table 1, 2.
69. Anna Stavrianakis and He Yun, *China and the Arms Trade Treaty: Prospects and Challenges* (London: Saferworld, 2014), 9.
70. Stavrianakis and Yun, 10.
71. Daniel Byman and Roger Cliff, *China's Arms Sales: Motivations and Implications* (Santa Monica, CA: RAND Corp., 1999), 31–35, 37–38, <https://www.rand.org/>.
72. Keegan Elmer and Echo Xie, "China Targets Tighter Controls on Its Growing Arms Trade," *South China Morning Post*, 25 December 2019, <https://www.scmp.com/>.
73. Jon Grevatt, "China's CSSC and Poly to Collaborate on Exports," *Jane's Defence Weekly*, 13 May 2019, <https://www.janes.com/>.
74. Lucie Béraud-Sudreau and Meia Nouwens, "Are Arms Exports a Tool of Chinese Foreign Policy?" *East Asia Forum*, 7 July 2018, <https://www.eastasiaforum.org/>.
75. Fleurant et al., *Trends in International Arms Transfers*, 2016.
76. Chung Min Lee, *Fault Lines in a Rising Asia* (Washington, DC: Carnegie Endowment for International Peace, 2016).
77. Wezeman et al., *Trends in International Arms Transfers*, 2018, 5.
78. Ridzwan Rahmat, "Algeria Commissions Second Chinese-Built C28A Corvette," *Jane's Navy International*, 16 March 2015; and Edward Wong and Nicola Clark, "China's Arms Industry Makes Global Inroads," *New York Times*, 20 October 2013, <https://www.nytimes.com/>.
79. Bahrain, for instance, has bought multiple rocket launchers (MRL) from China; Kuwait, artillery systems and armored personnel carriers (APC); and Oman, MRLs and APCs. SIPRI Arms Transfers Database.
80. Keith Bradsher, "Red Flags over Turkey-China Arms Deal," *The Hindu*, 24 March 2016.
81. Dan Blumenthal, "The Power Projection Balance in Asia," in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, Thomas G. Mahnken, ed. (Stanford, CA: Stanford University Press, 2012), 168, <https://books.google.com/>.
82. Richard A. Bitzinger, "A New Arms Race? Explaining Recent Southeast Asian Military Acquisitions," *Contemporary Southeast Asia* 32, no. 1 (2010): 50–69, <https://muse.jhu.edu/>.
83. Tai Ming Cheung, Eric Anderson, and Fan Yang, "Chinese Defense Industry Reforms and Their Implications for US-China Military Technological Competition," *SITC [Study of Innovation and Technology in China] Research Briefs*, Series 9 (2017-4), 28 February 2017, <https://escholarship.org/>.
84. Bitzinger and Raska, "Capacity for Innovation," 129–62.

# Strategy in the New Era of Tactical Nuclear Weapons

COL JOSEPH D. BECKER, USA

## Abstract

Post–Cold War strategic discourse, primarily among Russian strategists, has challenged the precept that nuclear weapons are not useful tools of warfare or statecraft. To reduce the likelihood that such ideas will ever be tested in practice, the US must openly address hard-case scenarios and develop a coherent strategy sufficient to give adversaries pause. This article posits that the key to successfully deterring the use of tactical nuclear weapons lies not in winning an arms race but in the clear articulation of a purpose and intent that directs all aspects of US policy toward the prevention of nuclear war and leaves no exploitable openings for opportunistic challengers. Further, an ideal strategy would be crafted to reduce—not increase—the salience of nuclear weapons in geopolitics. The article considers three possible approaches to a strategy for tactical nuclear weapons, but the most desirable and effective will be a “strategy of non-use” based upon credible and well-prepared alternatives to a nuclear response.

\*\*\*\*\*

The end of the Cold War ushered in a new era suggesting the possibility that nuclear weapons could become a relic of the past. Prominent leaders, including US president Barack Obama, campaigned vociferously for measures to abolish the world’s nuclear stockpiles.<sup>1</sup> However, instead of moving toward a world of “nuclear zero,” the US and Russia have proceeded with nuclear modernization and capability development, and even China is quietly expanding its nuclear arsenal.<sup>2</sup> Perhaps more disturbing, it is now tactical—not strategic—nuclear weapons driving the latest discussions. Of course, the term “tactical” is controversial when applied to anything as destructive as a nuclear weapon. Notable characteristics such as range, explosive yield, or intended target cannot decisively delineate between strategic and tactical aims.<sup>3</sup> Nevertheless, like Russia, the US continues to push forward with the development and fielding of nuclear weapon systems (e.g., the B61-12, “low yield” D5, and long-range standoff weapon) that can be configured to produce less explosive force than the 15-kiloton “Little Boy” dropped on Hiroshima in

1945.<sup>4</sup> Any weapon in this yield range that could conceivably support conventional forces or operations will qualify for the purposes of this discussion. Today, it appears that military thinkers are increasingly contemplating the possibility of limited nuclear warfare—a concept that had been nearly banished from the strategic lexicon, especially in the West.

The term “escalate to de-escalate” does not formally appear in Russian military doctrine, but a combination of provocative actions, insinuations, and policy pronouncements have led US officials to apply this label to Russian president Vladimir Putin’s strategic approach, as reflected in the 2018 Nuclear Posture Review (NPR).<sup>5</sup> Former USSTRATCOM commander Gen Kevin P. Chilton, USAF, retired, articulated this concern, describing how the threat or employment of tactical nuclear weapons might be used to discourage outside interference in a Russian campaign, especially in the event of a pending military setback.<sup>6</sup> The implication of this scenario is that a world actor (Russia in this case) might perceive utility in the employment of a tactical nuclear weapon under the assumption that the US is likely to blink in certain circumstances. While the US has responded to this threat, it has focused almost exclusively on achieving deterrence through matching or overmatching adversary capabilities. This tactic is both insufficient and potentially dangerous. Using Colin Gray’s 1979 treatise “Nuclear Strategy: The Case for a Theory of Victory” as a starting point, this article argues that effective deterrence requires articulating a coherent strategy for employing tactical nuclear weapons. Further, since the US would prefer never to see them used, the best strategy would address “escalate to de-escalate” scenarios while simultaneously demonstrating global leadership in the restraint of nuclear arms.

This discussion begins by reviewing Colin Gray’s argument and considering its implications for the present landscape of nuclear strategy. Next, it examines how US adversaries, especially Russia, are exploring new options for limited nuclear war and why this is dangerous. It then explores three options for developing a modern strategy with regard to tactical nuclear weapons employment. Ultimately—though difficult to implement—a *strategy of non-use* would be by far the most desirable option for the US in shaping its geopolitical environment and reducing the likelihood of a nuclear exchange.

### **The Case for a Theory of Victory**

Colin Gray’s seminal 1979 piece in *International Security* argues that the US had failed to articulate a coherent strategy during the Cold War for the employment of nuclear weapons.<sup>7</sup> This is not to say that the US



military had no plans in place for conducting a nuclear war, as it most assuredly did. However, policy pronouncements of the day reflected a confusing mix of mutually assured destruction (MAD) logic, overemphasis on pre-war deterrence, and a flexible response doctrine that relied on ambiguous threats of punishment—each containing questionable assumptions and logical fallacies. Collectively, they painted a muddled picture of a United States that was leaning almost entirely on the mere possession of nuclear weapons to provide a deterrent effect.

The crux of Gray's argument is that this approach lacked credibility because it overly emphasized the message that nuclear war was mutual suicide, and this invited adversaries to doubt US resolve to carry through on threats of retaliation (and its own suicide). Additionally, this ambiguity had a detrimental effect on US strategy. First, the fatalism of this approach discouraged sober reflection on how to win a nuclear war if forced to fight one. Second, the lack of a publicly articulated strategy made it impossible for civilian policy makers to effectively rationalize the nuclear force or contain DOD tendencies to engage in arms races. Gray's recommended solution to these problems was to develop and articulate a "theory of victory." While details and war plans would remain classified, the Soviet Union should be made to understand that the US undergirded its deterrence strategy with a clear and attainable path by which to come out on top in case deterrence failed. Not only would this message add credibility to deterrence efforts and prepare for any unavoidable conflict scenarios, it would also allow policy makers to rally around a coherent vision and re-source the nuclear arsenal appropriately.

It should be noted that Gray's position was not without controversy. Robert Jervis, one of his most notable critics, summarizes his own skepticism with this simple statement: "The problem . . . is not with the lack of a theory of victory, but with victory's impracticality."<sup>8</sup> While Jervis may have been skeptical that nuclear war could be won, his views largely aligned with Gray on the point that mixed messages sent by US policy makers regarding nuclear strategy undermined instead of enhanced the credibility of deterrence. Additionally, even after critically dissecting the prevailing nuclear strategy of the day, Jervis ultimately concludes his 1984 work *The Illogic of American Nuclear Strategy* by proposing that strong capability and unambiguous commitment would be the best path to deterring Soviet aggression.<sup>9</sup> It is difficult to understand how one could generate this prescribed resolve without developing and projecting a strategy clearly designed to win.

Fortunately for mankind, the Cold War came and went without a nuclear conflict. However, today's conflicts with Russia and an increasingly assertive China have allowed the US to modernize its nuclear weapons arsenal and expand its delivery capability for tactical nuclear weapons. US leaders have been unequivocal about the point that this expansion is a reaction to rising threats. The 2018 Nuclear Posture Review also states that the US has expanded its prerogative to use these weapons, including in response to "significant non-nuclear strategic attacks."<sup>10</sup> What remains unclear is how the US would actually use these weapons to attain its strategic goals if it were pushed to do so. The NPR primarily espouses a flexible response doctrine (based on the type of ambiguous threats of punishment criticized by Gray), stating that "tailored deterrence strategies communicate to different potential adversaries that their aggression would carry unacceptable risks and intolerable costs according to their particular calculations of risk and cost."<sup>11</sup> It specifically describes Russia as one of these potential adversaries and speaks to correcting misperceptions about the viability of gaining a strategic advantage through first use. But as the document proceeds, the basis for this "correction" appears to be a laundry list of the ways in which the US was expanding the capacity, flexibility, and reach of its nuclear forces.<sup>12</sup> Once again, the US is relying on the possession of nuclear capabilities as the primary basis for preventing nuclear war. Simply having weapons and vaguely threatening to use them—without articulating a strategy—falls short of establishing the credibility required for deterrence.

This article argues that the US needs a nuclear strategy that openly conveys a theory of victory in the modern world. Plans and strategies locked in the vaults of the Pentagon will neither effectively deter adversaries nor recapture the initiative in shaping the international landscape with regard to these weapons. If strategy, per the US Army War College, is "the relationship among ends, ways, and means," what would tactical nuclear weapons help the US achieve if they were ever used, and how might escalation be addressed?<sup>13</sup> At the same time, the prevention of nuclear conflict altogether certainly remains one of the foremost goals of US policy, so one must also consider the question, How does US strategy make nuclear weapons less relevant instead of more? Before examining these questions further, it is instructive to consider how the threat environment has evolved since the Cold War, particularly concerning the possibility of limited nuclear war.

### **Dangerous New Possibilities for Limited Nuclear War**

The end of the Cold War suggested the possibility that traditional paradigms of nuclear deterrence had outlived their usefulness. The

disintegration of the USSR, along with the consolidation and reduction of the Soviet nuclear arsenal, seemed to breathe life into the Reagan/Gorbachev vision of nuclear abolition.<sup>14</sup> However, a resurgent Russia and an ascendant China, with both countries expanding their nuclear capabilities, have returned the topic of nuclear deterrence to the forefront of the policy agenda. Russian president Vladimir Putin's provocations lend new relevance to the need for coherent strategy.

Gray warns in his 1979 commentary that "there could come to power in the Soviet Union a leader, or a group of collegial leaders, who would take an instrumental view of nuclear war."<sup>15</sup> The Cold War saw no such development, but since the turn of the century, Russian strategic thought has been leaning in this dangerous direction. Jacob Kipp, in his chapter "Russian Doctrine on Tactical Nuclear Weapons: Contexts, Prisms, and Connections," describes how Russian strategists have applied their own frameworks to Western conceptions of the "generations of warfare." Russian scholar Alexei Fenenko, in particular, authored an influential article in 2004 advocating the use of tactical nuclear weapons in precision strikes, which he believed could be useful in de-escalating a conflict before it expanded and risked general nuclear war. This concept would be part of a "sixth generation of warfare," and it questioned Western shibboleths about mutually assured destruction with regard to the nuclear threshold.<sup>16</sup> Fenenko also wrote a 2009 article clarifying Moscow's own "flexible response" doctrine and defending a then-recent announcement by the Kremlin repudiating the doctrine of "no first use."<sup>17</sup>

It should not come as a surprise that Russians today would treat the concept of MAD with skepticism. Lawrence Freedman, in his book *The Evolution of Nuclear Strategy*, explains that Soviet leaders—especially in the military—never fully embraced this concept, nor did they consider themselves "deterred."<sup>18</sup> According to Freedman, "The Russians did not deviate from the traditional view that the role of strategy was to devise a means of winning future wars, and the role of military planning was to prepare the necessary forces." Their focus was war fighting, not deterrence per se. The ability to win would provide the coercive capacity needed to deter.<sup>19</sup>

More striking, however, is the contrast between Fenenko's writing and Cold War Soviet military doctrine. A leading Cold War postmortem by the BDM Corporation reveals that Soviet nuclear doctrine of that time was largely devoid of concepts like escalation control, crisis management, and intrawar escalation. While not completely ruling out the possibility of a limited war, the doctrine did not emphasize planning for one and thus had little basis for a "flexible response" doctrine.<sup>20</sup> Fenenko, on the other

hand, not only champions this Western concept but also proffers a strategy of escalation dominance reminiscent of Herman Kahn.<sup>21</sup> His proposed employment of tactical nuclear weapons bears closer resemblance to the US Army doctrine of the early 1950s than anything from Soviet history.<sup>22</sup>

There is considerable controversy over what escalate to de-escalate would look like in practice, especially in terms of nuclear weapons. Moscow's rhetoric has insinuated far more than it has actually stated. What it shows, however, is that Russia is determined to challenge US resolve about its security commitments, and it might very well flex its muscles to the point of testing the nuclear threshold when it perceives an advantage. The Pentagon is most concerned that Russia may invade one of its regional neighbors and either threaten use of or employ a nuclear weapon to discourage outside interference.<sup>23</sup>

Unlike a dispute between India and Pakistan, where the tit-for-tat exchange might be brutal but relatively straightforward, this scenario begs a complicated question as to how the US could respond. Even assuming the target of aggression was a NATO ally, would the US retaliate with a nuclear strike? If so, where and what would it strike? Would a retaliatory strike in the disputed country be more of a punishment to Russia or the local population caught in the middle? Conversely, would the US be willing to escalate the situation by striking a target on Russian soil? Doing so would certainly risk the onset of World War III. Could the US afford to send a conventional ground force? Force projection along the Russian border would be a difficult and costly venture. US forces would have to prepare for the possibility that they would be entering history's first real nuclear battlefield. Even without the introduction of tactical nuclear weapons, there is no guarantee that such a ground or air campaign would avoid escalation to a full-scale conventional or nuclear war with Russia. Finally, how much allied support could the US expect in any of these scenarios? If NATO members were to balk at the costs of a war, how long could the alliance endure? There can be little doubt that this conundrum is what prompted Russian strategists to envision utility for tactical nuclear weapons.

Another disturbing possibility is that the principle behind this approach could be extended beyond Russia's immediate neighborhood. What if the Russians, fearing expulsion by US forces, had brought tactical nuclear weapons to Syria? While they may have tolerated limited aggression against their forces, any existential threat could have been met with the counter-threat of a nuclear strike, making them essentially impervious. Yet again, what if Russia's next expeditionary adventure is even more controversial or ambitious, and it decides to include nuclear weapons in its mobile defense

package? Its forces could lodge themselves into a conflict or region such that dislodging them would become almost completely infeasible.

As troubling as this scenario might sound, the precedent it would set could be still more dangerous. China has demonstrated consistently that it intends to expand its area of influence, especially in Southeast Asia and the Pacific. It has not yet threatened the use of nuclear weapons, and in all probability, it does not see a need at present. But if the example were set by Russia that tactical nuclear weapons can successfully bolster expansionist goals, US hopes of developing China as a peaceful and constructive partner on the world stage might be vastly complicated. The need to avoid these difficult and dangerous scenarios serves to highlight the importance of developing an articulable strategy for tactical nuclear weapons.

### **Options for a Modern Theory of Victory**

The US answer to Russia's developments in its tactical nuclear force has apparently been a response in kind, modernizing its own force and developing new delivery vehicles like hypersonic rockets and ground penetrators. However, this is exactly the approach Gray warns against. Developing nuclear weapon capabilities without a clear strategy is potentially wasteful and dangerous. But how can the US develop a coherent strategy for hard-case scenarios—where at least one side believes that nuclear weapons can be successfully employed in a limited fashion without undue risk of full-scale escalation? Three potential options exist. The first is to bolster and rely on conventional deterrence to preclude the emergence of a limited-use scenario. The second is for the US to articulate a coherent strategy that incorporates tactical nuclear weapons. The third is to develop a strategy of non-use, or a credible nonnuclear response.

#### ***A Purely Conventional Approach***

One way to respond to the challenge of tactical nuclear weapons is developing a strategy obviating their need altogether. Robert Haffa explores this option in his *Strategic Studies Quarterly* article “The Future of Conventional Deterrence: Strategies for Great Power Competition.” He indicates that the key to avoiding great power conflict is to develop a conventional force posture formidable enough to deter aggression by potential adversaries. Such a force posture would demonstrate that the US, while retaining its nuclear capabilities, is not dependent on them. Haffa also posits that a conventional deterrent is more credible than a nuclear deterrent because it removes the possibility that the US might be self-deterred

by the gravity of a decision to employ nuclear weapons. While Haffa never explicitly argues against developing strategies for the use of nuclear weapons, his work clearly implies that the US would be safer if national security relied primarily on a robust conventional force that allowed it take nuclear weapons off the table in planning for likely conflict contingencies.<sup>24</sup>

Applying Haffa's logic at the macro level, the US would deter and, when necessary, respond to aggression by adversary nations with an overmatch of conventional military capabilities. This approach would paint the US as a squarely "status quo" power, responding to threats against its allies or interests. Deterrence would seek to prevent revisionist powers from upsetting the stability of, for instance, existing borders, power structures, and economic relationships, therefore reducing the likelihood of a nuclear war. Victory, in the case of conflict, would then be defined by the condition where a region or an issue under question has been returned to its original state, and possibly made more secure in that position. At the regional level, Haffa's logic would require the US to examine a wide range of the most likely potential conflicts—which the Department of Defense certainly does on a daily basis—and to seek a conventional overmatch for each contingency. Haffa himself provides one application of this process by briefly considering what the US might require to conventionally deter Russia from aggression against the Baltic states.<sup>25</sup>

While his approach allows for a coherent strategy, it is problematic for a number of reasons. First, it relies on conventional deterrence to prevent nuclear war. According to this logic, conventional parity and overmatch would prevent the kind of conflict that might spark a nuclear exchange in the first place. But as Haffa readily admits, conventional deterrence often fails.<sup>26</sup> What then would prevent either side from crossing the nuclear threshold if it perceived an advantage? Since neither side can unilaterally restrict the conflict, both sides must be prepared to employ their weapons effectively.

The second problem with a purely conventional approach is its overreliance on the status quo to underpin its theory of victory. Henry Kissinger describes the concept of world order as an inherently evolutionary process, shaped by the incessant challenges of both contested ideas of legitimacy and shifting power relations.<sup>27</sup> All manner of circumstances and interests are subject to change over time. Haffa's approach—in a manner reminiscent of the Cold War—relies heavily on alliances for the forces required to deter a great power adversary, especially Russia. Alliances, however, depend on relationships and commitment, both of which are variable according to domestic politics on either side. Additionally,

America's partners must retain the capability to add military value in a conflict outside their borders—an assumption under increasing question. Further, conflicts are rarely black and white. Most of the Russian aggression since the end of the Cold War has occurred on the pretext that political crises have necessitated foreign intervention (even if these crises were covertly manufactured by Russia itself). If a real political crisis were to occur in the Baltic states (regardless of who started it), it would beg the question of who should rightfully intervene. John Mearsheimer, from a perspective of offensive realism, challenges the entire concept of a status quo, stating that “status quo powers are rarely found in world politics, because the international system creates powerful incentives for states to look for opportunities to gain power at the expense of rivals, and to take advantage of those situations when the benefits outweigh the costs.”<sup>28</sup> A theory of victory that relies primarily on defending the status quo is working against the tide of history.

The third problem with a purely conventional approach to deterrence is that it requires a country to periodically use force to demonstrate its capability and resolve.<sup>29</sup> This stipulation exposes an internal inconsistency within the concept itself. When a nation employs its military, it not only displays potency but also tips its hand. America's wars against Iraq and Afghanistan awed the world, but they also telegraphed the strengths and limitations of US military power. In a manner consistent with the “security dilemma” of international relations, applications of US power have increased the insecurity of potential rivals and prompted more aggressive and effective balancing. Additionally, as the US has learned time and again, employing force incurs unintended commitments. Quagmires in Afghanistan, Iraq, and Syria have proven a tremendous drain on military manpower and resources. One could easily argue that instead of enhancing America's conventional deterrence capability, military campaigns have eroded it.

Perhaps the greatest problem with the purely conventional approach is its impracticality and even unattainability from a resource perspective. No great power has ever maintained continuous overmatch on all fronts. An effective deterrent in the Baltics might require a commitment as high as 225,000 ground troops, either forward deployed or rapidly deployable, between the US and its allies.<sup>30</sup> Deterrence of China would require a network of new bases and forward-deployed troops around the Pacific region. All ground forces of the US military would have to be increased, along with the entire infrastructure for rapid deployment. The US would have to maintain unrivaled air superiority and global strike capabilities in an age

when missile and drone technology is eroding this advantage. It would also need to simultaneously and rapidly defeat multiple echelons of a near-peer adversary's military capability, without considering the counter-efforts and capabilities that the US would face. The cost of such a strategy, both fiscally and politically, would be prohibitive. Further, because of the "security dilemma," such a buildup might actually spark one of the wars it would seek to prevent.

These points of contention should not be taken as an argument that conventional forces are obsolete or that conventional deterrence does not have an important place in national defense. What they do suggest is that when dealing with nuclear-armed rivals or potential adversaries, a conventional military solution will be insufficient to prevent nuclear war, and it would be impractical to base nuclear strategy on the conventional defense of the status quo. This path will not allow the US to bypass difficult questions regarding tactical nuclear weapons.

### *Integration of Tactical Nuclear Weapons*

By most accounts, the advent of nuclear weapons brought a paradigm shift in theories of warfare. These weapons were different. For many thinkers, including Kenneth Waltz, instead of revolutionizing conventional warfare, nuclear conflict became a class unto itself.<sup>31</sup> If a war were to cross the nuclear threshold, the game would change, and conventional capabilities would become largely irrelevant. In spite of these views, the continued development of tactical nuclear weapons reminds us that the possibility of limited nuclear war has never been absent from the strategic landscape. Moreover, as global bipolarity and America's subsequent "unipolar moment" have both eroded with time, the strategic constraints that previously shaped the nuclear era might be up for reconsideration.<sup>32</sup>

The second path to a tactical nuclear weapons strategy would involve integrating these weapons into the existing force. This approach apparently matches the direction observed in US adversaries, such as China, Russia, and North Korea. It would necessitate accepting the possibility of limited nuclear war, although it would not necessarily be offense oriented. In any case, the US could still eschew first use. The initial challenge with such an approach is that victory would be highly context specific. Unlike the Cold War theory of victory that Gray suggests, a modern strategy would have to incorporate a wider range of adversaries and potential scenarios. Ideally, tactical nuclear weapons would find their place within a coherent grand strategy. Regardless, they would be assigned in support of specific, preexisting policy objectives. The important consideration is that



the addition of a nuclear dimension would also increase the gravity of the discussion surrounding the policies themselves.

Consider three possible points of entry for tactical nuclear weapons into US strategy. The first is comprehensive integration. Tactical nuclear weapons could be used to augment conventional forces. This was the US military's initial approach to nuclear weapons strategy in the 1950s. Though opposed to America's first use of the atomic bomb in World War II, General MacArthur strongly advocated atomic strikes during the Korean conflict, and the military requisitioned new warheads and conducted test runs for this contingency.<sup>33</sup> While Truman refrained from authorizing the strikes in Korea, the military continued to develop this concept. Nuclear weapons then became a cornerstone of national defense under the Eisenhower administration, which found itself caught between a growing Soviet threat and the exigencies of domestic politics. These weapons seemed like an ideal way to fill the gap in conventional force ratios without breaking the bank.<sup>34</sup>

Eisenhower's strategic approach paved the way for the embrace of tactical nuclear weapons, and it envisioned their use in any future conflict with the Soviets. By the middle of the 1950s, nuclear weapons were fully integrated into military forces and strategy. In December 1953, the chairman of the Joint Chiefs of Staff was quoted as saying, "Today atomic weapons have virtually achieved a conventional status within our armed forces."<sup>35</sup> Support for this approach also came from some surprising quarters. Scientists such as J. Robert Oppenheimer, an early advocate of nuclear arms control, actually favored the development of tactical nuclear weapons as a way to shift focus away from hydrogen bombs and bring "battle . . . back to the battlefield."<sup>36</sup>

The incorporation of tactical nuclear weapons as a form of heavy artillery led to radical changes in the structure and doctrine of the military force. Andrew Bacevich traces this evolution in his book *The Pentomic Era*.<sup>37</sup> In hindsight, Bacevich explains, the Army's "pentomic" concept was a dismal failure. This new style of fighting turned the conventional principles of warfare on their head and created serious problems with command and control. It quickly became apparent that this doctrine was ideal only for a specific, unlikely scenario of nuclear warfare. Even more, the Army's assumptions about its ability to fight in an irradiated environment were almost laughable, sometimes wishing away the effects entirely.<sup>38</sup> While the pentomic concept proved little more than a costly detour in the history of the Army, many of the weapons it developed remained in the inventory and continued to serve a strategic role throughout much of the Cold War.

The question for today is whether conditions have changed that might make it practical or desirable to reincorporate nuclear weapons into conventional doctrine. To begin with, advances in missile and long-range drone technology—along with the fledgling development of hypersonic delivery vehicles—may obviate the need to issue nuclear weapons directly to troops. These advances have already made the weapons more accurate and effective than their predecessors have. Also, the authority and capability to launch these weapons could be far more tightly controlled than would have been possible during the Cold War. Another advantage of comprehensive integration is that it would prompt the military to update its doctrine, training, and equipment for nuclear contingencies that might happen anyway. Bifurcating conventional and nuclear conflict has allowed the US military to continue neglecting preparation for combat in irradiated environments. Demonstrating preparedness to fight under such conditions could also enhance deterrence, as adversaries would not be able to utilize radiation for area denial purposes.

However, in seriously considering the option of comprehensive integration, the factors that have not changed are more problematic than those that have. Even with new technologies and global reach, the idea that integration can be accomplished while maintaining tight, centralized control of nuclear weapons runs counter to the principles of war. Robert Peters, Justin Anderson, and Harrison Menke, for instance, argue for full integration of tactical nuclear weapons into planning and exercises for regional conflicts, but their 2018 article begs the question of when and how the authority to use these weapons would be delegated to military commanders. Commanders cannot successfully prosecute campaign plans in a complex, dynamic environment if they do not have tactical control of the assets upon which their plan depends. This type of delegation, however, requires the dangerous assumption that escalation could be limited to the geographic theater of conflict.<sup>39</sup>

Thomas Schelling wrestled with the problem of escalation and suggested that deterrence might continue to operate even during the course of a nuclear conflict, ultimately limiting the scope, but it has never been clear how this would play out in practice.<sup>40</sup> Supposing that nuclear weapons were treated strictly as artillery for an otherwise conventional campaign, what would prevent the losing or disadvantaged side from simply opting for bigger artillery? Is it logical to assume that a nation would choose to sacrifice a core interest when escalation options remain? Some might suggest that restraint would hold in peripheral conflicts, but the Cold War demonstrated a dampening effect on the number and scope of

these conflicts precisely because of the specter of nuclear war. Neither superpower was willing to test the limits because both were uncertain of the outcome. Herman Kahn, one of history's most influential theorists regarding escalation, likens the assumptions required for nuclear brinkmanship to attempting to play a "limited game of 'chicken.'" Further, he states, "To rely . . . on slow, rung-by-rung escalation in international crises is a dangerous strategy."<sup>41</sup>

Finally, the argument that Russia and China may be considering some elements of comprehensive integration is not sufficient justification for the US to follow suit. International norms and conventions such as the Non-Proliferation Treaty (NPT) still constrain the spread of nuclear weapons and the behavior of nuclear powers. Although they are flouted in some cases, they are followed in most. A belligerent approach by the US might inadvertently undermine this fragile regime. There are still options for preventing a dangerous spiral of escalation between the existing nuclear powers, but the likelihood of a nuclear war would increase if the US were to move toward a more aggressive stance.

Less drastic than comprehensive integration, another point of incorporation for tactical nuclear weapons might be termed *defensive integration*, or a tripwire concept. A primary example of defensive integration is the US defense of Western Europe during the Cold War. When the Eisenhower administration first developed its concept of massive retaliation, no threat was higher on its list of concerns than that posed by the Soviets against European allies. Bernard Brodie, one of the early academic theorists of nuclear deterrence, personally advocated the employment of tactical nuclear weapons to "redress what is otherwise a hopelessly inferior position for the defense of Western Europe."<sup>42</sup> As the Cold War progressed, "massive retaliation" gave way to "flexible response," and the use of tactical nuclear weapons was never guaranteed under this approach, but always possible—according to the needs of US policy makers. In fact, these weapons, which peaked at more than 7,000 tactical warheads, largely served a political role in assuring allies of US commitment to their defense.<sup>43</sup>

The foundation for defensive integration as a theory of use for tactical nuclear weapons is area denial. If an adversary crosses a specified line, it risks triggering a nuclear response. As with comprehensive integration, advances in technology would largely reduce the need for the forward basing of nuclear weapons, making the implementation of such a strategy potentially simpler than before. However, any intercontinental launch risks the possibility of sparking a general nuclear war, as opponents will be

hard-pressed to distinguish tactical from strategic warheads or predict impact points with speed and accuracy.

The key problem in considering defensive integration for area denial is the question of *whose area*. The idea that nuclear weapons might be used to protect one's homeland against foreign invasion has become relatively uncontroversial. What is very controversial is the concept of a "near abroad." Russia and China have been increasingly assertive in defining what they believe is their own sphere of influence. In Russia's case, the concept of escalate to de-escalate was envisioned for the express purpose of isolating a conflict with one of its neighbors. The fact that NATO has expanded to the Russian border directly challenges Russia's claim to its near abroad. Depending on one's point of view, this move might be appropriate, but it is a complicated one. If there was a question mark as to US willingness to use nuclear weapons in the defense of Western Europe, how much more might this resolve be questioned with regard to the Baltic states? Likewise, would the US risk a general nuclear war with China over territory controlled by the Philippines? Defensive integration is a theory of use based upon protecting the status quo, but it does not deal well with situations where this status quo is already contested. Therefore, a defensive integration approach would largely perpetuate the cycle of uncertainty.

A third approach to a theory of use for tactical nuclear weapons will be labeled *specialized uses*. In this approach, tactical nuclear weapons may be considered for situations in which they are uniquely suited as tools of warfare. A current example is bunker busting. This relatively new application for nuclear technology did not exist during the Cold War. The US military began developing ground-penetrating missiles in the 1990s in response to revelations regarding deeply buried nuclear facilities in North Korea and Iran. It asked Congress to fund the development of nuclear versions in 2002.<sup>44</sup> Since then, the US Department of Defense has advanced its technology for both nuclear and nonnuclear ground penetration.<sup>45</sup>

From the standpoint of a theory of use, the logic of specialized uses is relatively straightforward. The US will win any conflict because an adversary has nowhere to hide. But are nuclear weapons both necessary and desirable for this purpose? While fully comparing these classified technologies is impossible, nonnuclear ground penetrators might be sufficient to the task. Conversely, the technology of tunneling and fortification continues as well and may challenge the limits of a conventional option. The question of desirability is even more complicated. On one hand, the collateral damage might be low in some conditions (although the environmental impacts are difficult to predict). On the other hand, this does not

mean that tactical nuclear weapons' use would not alter the geopolitical environment. Most nations would likely condemn their employment, and some nuclear actors might be emboldened to challenge nuclear taboos in their own circumstances. Furthermore, unless the US removes its unilateral moratorium on nuclear testing, the capability and effects of these weapons will remain unproven.<sup>46</sup> For all these reasons, some US policy makers are squarely against the concept of this type of weapon, and former representative David Hobson (R-OH) is quoted as saying, "What worries me about the nuclear penetrator is that some idiot might try to use it."<sup>47</sup>

Another consideration is the effect nuclear penetrators have on the overall concept of nuclear deterrence. Nuclear weapons and their associated development programs have previously been considered impervious when buried deep within hardened bunkers. The possibility of destroying these bunkers means that both an adversary's first- and second-strike capabilities can be held at risk. As pointed out by Kier Lieber and Daryl Press in their 2017 article for *International Security*, the Cold War concept of nuclear deterrence was based largely upon the premise that neither side could feel confident about eliminating the other's nuclear arsenal with a first-strike attack. If both sides retain a secure second-strike capability, then neither opponent feels that it must attack first to avoid being disarmed. These authors' concern is that expanding technologies for finding and destroying second-strike capabilities would undermine deterrence and make a world of nuclear-armed actors much less safe.<sup>48</sup> Thus, while nuclear penetrators may have been designed with countries like Iran and North Korea in mind, they pose a threat to all nuclear powers, especially Russia. Regardless of whether specialized uses are retained independently or in combination with comprehensive or defensive integration, a clearly articulated strategy is necessary to provide both the warnings and the reassurances required to turn these weapons from tools of provocation into instruments of effective deterrence.

### **A Strategy of Non-Use**

The 1983 movie *WarGames* carries a simple and compelling message—the only way to win the game of thermonuclear war is not to play. But the neat simplicity of this wisdom has always been undermined by the question, What if the other side decides to play anyway? While nobody wants a nuclear war, how can you convince your adversary not to play the game if it suspects you might not be willing to retaliate in kind? This is the problem that Russian strategists have attempted to exploit: considering provocations that would leave the West in checkmate, unable or unwilling

to respond. Might it still be possible to win without playing, though, at least by the adversary's rules? An effective strategy with an articulable theory of victory need not necessarily require a nuclear response. By presenting a coherent strategy of non-use, the US can likely deter the employment of tactical nuclear weapons in a scenario involving calculated escalation for the purpose of de-escalation; if deterrence fails, it can secure its interests without resorting to nuclear war. If an adversary can be made to understand that the employment of a tactical nuclear weapon will clearly result in the unpalatable choice between strategic loss or general nuclear war (strategic loss on a grander scale), then the perceived advantage of escalate to de-escalate will disappear.

How would deterrence be conceived in such an approach? A strategy of non-use begins with sending a general message that no government will ever be allowed to profit from a nuclear attack, regardless of whether it is answered in kind. Then, if deterrence fails and a country uses a nuclear weapon in what it believes to be a limited fashion, the US should lead the international community to turn its back so sharply and decisively on the aggressor that, in the long-term, no other country will again be willing to follow this example. Of course, nuclear war is always possible in any scenario irrespective of the best strategic approach. A strategy of non-use designed to prevent the clever employment of a tactical nuclear weapon should also be underpinned by a full range of nuclear retaliatory options that are not limited to tit-for-tat exchanges, leaving the initiative with the aggressor. Moreover, it should be nested within an articulated strategy for general nuclear war. The specifics of such an overarching strategy transcend the scope of this work. However, one would envision destroying the military and political capacity of an aggressor to make war, ensuring such a thorough defeat that it has no other interest but to rebuild its society as a just and peaceful member of the international community.<sup>49</sup>

There are several key requirements that will allow a strategy of non-use to succeed. First, it cannot be based upon merely defending the status quo. Change is inevitable, and the US should lead the international community in asserting that nuclear weapons will never stem the tide of change or effectively resolve any conflict. Additionally, it needs to be widely recognized that any act of nuclear aggression will alter the global order as it is currently understood. A nonnuclear response robust enough to deter an attack must similarly change the world, making it a very uncomfortable place for the aggressor—even at the cost of sharing discomfort across the international community. Some of the changes would be permanent, with second- and third-order effects for the way international

business is conducted. Accomplishing them would require the broad propagation of new standards and norms, a process that would involve challenges. With US leadership, it would be possible.

Second, a strategy of non-use must incorporate tailored approaches toward specific actors and scenarios. A one-size-fits-all solution will be unlikely to deter every potential adversary since the vulnerable points of pressure will shift over time. The US is in some ways fortunate because Russia is currently the only state that appears readily positioned to exploit a gray area in the framework of global deterrence. The possibility of nuclear aggression by North Korea or (eventually) Iran is terrifying to contemplate, but it would almost certainly invite a swift nuclear response designed first to disarm and second to topple the ruling regime. Few would doubt US resolve against these adversaries. India and Pakistan could wage nuclear war against each other, but again, it is difficult to imagine the scenario where a gray area might invite an unanswerable nuclear attack. China, on the other hand, could potentially follow Russia's model and prove much harder to deter, especially within its sphere of influence. It is unlikely that China would find such an option advantageous during its current state of ascendance, but conditions could change in the decades to come. Therefore, engaging the process of crafting an effective deterrent against Russia could pave the way toward reducing a long-term danger. Ideally, China should be treated as a partner in inoculating the world against this type of threat.

Third, the nonnuclear response to a nuclear attack needs to be not only punishing but defeating. Thomas Schelling describes "punishment" as the basis for nuclear deterrence, using the threat of overwhelming violence as leverage for coercion.<sup>50</sup> In this vein, a strategy of non-use would eschew the extreme violence of a nuclear attack—at least in some cases—but it must promise a maximum level of pain and disruption to be similarly effective. Unfortunately, the threat of punishment may not be enough to deter aggression. Victory should leave the opponent vanquished. It means permanently altering the game so the same actors can never use the same strategy under similar conditions again. The response required to defeat an adversary without resorting to a nuclear attack would likely include some conventional military component, but more importantly, it should integrate all the elements of national power across a wide network of international partners. Bear in mind that a strike with a single tactical warhead would conceivably destroy a battalion, a command node, a couple of ships, or perhaps some aircraft, but a coordinated nonnuclear response could be far more costly in strategic terms. It should fundamentally alter the condi-

tions under which an aggressor government and its societal elites engage with both their domestic population and the surrounding world.

In the case of Russia, several possibilities exist. First, all financial assets belonging to any Russian citizen outside its borders should be frozen and subject to forfeiture, most likely to the country in which they are held. Russia is particularly vulnerable to this approach because insecure property rights within its borders prompt elites to put their money elsewhere. Of course, in a world of laws, norms, and complex relationships, this proposal would be complicated to implement. A response like this would take years of diligent, coordinated groundwork to prepare. This effort would also be contested as Russia would undoubtedly move to reduce its vulnerability. The process would cause positive and negative evolutionary changes to the international system of economics, but it would certainly elevate the issue of nuclear deterrence internationally and integrate it into other fields of discussion.

Second, the US and its partner nations could cripple the export of Russian oil and gas. This action should not be accomplished without considerable planning and preparation. It would involve significant short-term pain, especially for those countries currently dependent on Russia for natural gas. If the US could accommodate its allies with alternative sources of energy and leverage allied support, it would send a powerful message to the Russian government and ruling elites.

Third, the US and its partners could institute a travel ban on all Russian citizens and deny air traffic to and from Russian territory. Fourth, the US could spearhead an effort to have Russia permanently removed from the United Nations Security Council. Fifth, the US should prepare a menu of potential conventional military options focused on Russian interests. It may include deployments into Russia's near abroad, where attacks at its periphery could prove more damaging. For instance, Russian naval vessels outside of home port could be held at risk and captured or destroyed under certain conditions. The military portion of this response may or may not take place in conjunction with a conventional conflict over territory (such as a ground incursion into the Baltic states), but the key difference in the case of a nuclear event is that Russia's ability to act as a great power outside its borders should be significantly degraded.

These are but a few of the potential options. The common theme is that, human cost aside, it is entirely possible to exceed the punishing effects of a limited tactical nuclear response without using nuclear weapons. The price of doing so involves a degree of pain to the US and its allies as well. This toll is one of the primary reasons why an articulable strategy is



important. Not only would it send a clear deterrent message, it would also be a tool for the US to gauge the requirements of its own approach realistically and galvanize the domestic and international support necessary to implement such a strategy. Many critics might point to a case like Iran and claim that sanctions and other economic measures, in particular, do not work. The response to this argument is that neither the US nor any other country has generally been willing to endure a great deal of pain in applying sanctions that really bite. The point at which pain becomes reciprocal has always been the sticking point for rallying domestic and international support. The US cannot solicit the support it needs for such a strategy without an aggressive diplomatic and public engagement campaign supported by a clearly articulated strategy of non-use. Undoubtedly, this exercise in coalition building would be more difficult than simply planning a nuclear response. However, pretending that one is going to use a nuclear weapon and then being unable or unwilling at the moment of need would be the worst of all worlds.

A final cost to consider regarding a theory of non-use is that it would inherently bind the US to a commitment not to use its own nuclear arsenal for a first strike. Some strategists will likely chafe at this inflexibility. But it suffices to say that the preemptive use of nuclear weapons has been highly controversial. The US would also have to forego its stated prerogative for a nuclear response to either a cyberattack or an attack with another form of weapon of mass destruction. Again, this constraint invokes a discussion outside the scope of this work, but America must decide if, while possessing the world's greatest conventional force and a host of cyber capabilities, it really needs nuclear weapons to respond to these contingencies. It does not.

An advantage to the US for allowing itself to be so bound is that it could credibly begin new initiatives for arms control. In fact, the groundwork required for building a nonnuclear response could potentially become the basis for a new arms control regime. The framework designed to deter Russia could eventually include Russia itself, and it would almost necessitate cooperation with the Chinese. If nothing else, the US would resume a leading role in shaping global norms and expectations for the use of nuclear weapons, and this could have significant positive results.

Some will undoubtedly argue that taking extreme measures to isolate Russia internationally and pressure its leadership from without and within would only risk inspiring irrational and unpredictable behavior—possibly leading to a general nuclear war instead of preventing it. However, it must be noted that these measures would only be taken in response to a nuclear

attack—one of the most reckless acts possible in the modern world. Since the next step on the ladder of escalation could result in full-scale nuclear war, extreme measures would be more than justified. It would be wise to establish off-ramps that allow for de-escalation, but just as the nuclear genie cannot be returned to the bottle, neither should Russia (nor any other actor) be completely restored if it were to choose such a course of action. The consequences will not be quickly forgotten and should not be quickly forgiven.

Beyond the difficulty required to implement a theory of non-use, one could also argue that this approach is just another form of conventional deterrence using a wider set of national power instruments. To an extent, this is true. Tools of diplomacy, information, and economics would take the lead, while military power would perform a supporting role (unless the conflict escalates on a military basis). This strategy addresses a limited set of hard-case scenarios (i.e., not an attack on core US interests) where a nuclear response would be questionable. If escalation could not be contained, the full range of nuclear response options would remain in play. Additionally, while a theory of non-use would still rely heavily on commitments from partner nations, the required contributions would be more political and economic in nature, and less military, making them far more credible to an adversary. Most importantly, such an approach would reflect a fundamentally different character in the way the US relates to other nations and to global order in general. Whereas the conventional deterrence approach would require an expansion of the US global military footprint and exacerbate concerns regarding American imperialism, a strategy of non-use would foster diplomatic and economic ties in a cooperative effort to address an existential threat to humanity. Not only would such a policy shape the global environment in a more positive direction, but the effort required would shape the US as well—ideally into a more suitable leader for the free world.

## Conclusion

While this article advocates the development of a *strategy of non-use* for tactical nuclear weapons, it cannot replace all other forms of strategic nuclear deterrence. A nuclear attack impacting the US homeland or core national interests would warrant a nuclear response in most conceivable cases, and the US should express its resolve in the clearest possible terms. America should build a nonnuclear response apparatus that precludes the need to automatically respond in kind to nuclear aggression outside the realm of its core interests, but it should always be prepared to escalate to

nuclear war if necessary. Additionally, while the 2018 NPR points to multiple, situation-specific “tailored strategies,” these should be more than a list of capabilities. They should articulate to friend and foe alike how the US will use (or refrain from using) its new weapons for victory if so required. Elements from the conventional approach—along with *comprehensive* and *defensive integration*—may find an appropriate place, and even *specialized uses* might be considered but with great caution.

The key lesson is that effective nuclear strategy includes publicly articulating a logical roadmap between means and ends, supported by policy makers and respected by America’s adversaries. Some might argue that this view is escalatory, inviting a bellicose response, but the US has already ceded initiative to adversary states by falling into an arms race approach. An effective strategy should anticipate and effectively shape the response it will elicit, thus reducing uncertainty for all parties. It should also be considered that the tacit framework now serving as the public face of US nuclear policy reflects the contested nature of political opinions and even democracy itself. Policy makers, along with the American public, have a wide range of views about nuclear weapons. To some extent, ambiguity allows the military to avoid paralysis within a contentious political milieu. However, by keeping the logic that underpins US strategy vague, unspoken, or highly classified, the defense establishment can summarily dismiss its critics and perpetuate abiding habits like arms races. In doing so, it avoids critical self-examination.

Unfortunately, errors in logic create exploitable weaknesses that could inadvertently lead to nuclear war. The US should address these weaknesses now, in a time of relative peace. If nuclear strategists draw the wrong lessons or fail to answer difficult questions, the world will become a more dangerous place. Just as articulating a strategy for tactical nuclear weapons is likely to prompt America’s adversaries to respond in kind, projecting vagueness, ambiguity, and logical inconsistency can have the same effect. **SSQ**

**COL Joseph D. Becker, USA**

Colonel Becker is an active-duty Army officer and a PhD fellow in the Army Strategic Planning and Policy Program (ASP3). He currently studies political science at Johns Hopkins University. His previous assignments include service as a graduate faculty instructor at the National Intelligence University.

**Notes**

1. “Nuclear Disarmament: Obama’s Lonely Quest,” *The Economist*, 22 June 2013, 33, <https://www.economist.com/>.

2. David Axe, "China Just Practiced Launching a Nuclear Weapon," *The National Interest*, 24 January 2019, <https://nationalinterest.org/>.
3. USSTRATCOM commander Gen John Hyten commented in September 2017, "I think it is actually a very dangerous term to use, because I think every nuclear weapon that is employed is strategic." Tara Copp, "Mattis: Use of Tactical Nuclear Weapons Discussed with South Korea," *Military Times*, 18 September 2017, <https://www.militarytimes.com/>.
4. Ankit Panda, "First New US Low-Yield Submarine-Launched Ballistic Missile Warhead Produced," *The Diplomat*, 14 March 2019, <https://thediplomat.com>.
5. Amy F. Woolf, *Nonstrategic Nuclear Weapons*, CRS Report RL32572 (Washington, DC: Congressional Research Service, 6 September 2019), 25–26, <https://fas.org/>.
6. Kevin P. Chilton, "On US Nuclear Deterrence," *Strategic Studies Quarterly* 11, no. 4 (2017): 6–7, <https://www.airuniversity.af.edu/>.
7. Colin Gray, "Nuclear Strategy: The Case for a Theory of Victory," *International Security* 4, no. 1 (1979): 54–87.
8. Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca: Cornell University Press, 1984), 182.
9. Jervis, 110–11, 168–70.
10. Office of the Secretary of Defense, *2018 Nuclear Posture Review [Final Report]* (Washington, DC: Department of Defense, February 2018), 21. <https://media.defense.gov/>.
11. Office of the Secretary of Defense, viii.
12. Office of the Secretary of Defense, xii.
13. Robert H. Dorff, "A Primer in Strategy Development," in *U.S. Army War College Guide to Strategy*, eds. Joseph R. Cerami and James F. Holcomb, Jr. (Strategic Studies Institute, February 2001), 11, <https://ssi.armywarcollege.edu/>.
14. Martin Senn and Christopher Elhardt, "Bourdieu and the Bomb: Power, Language and the Doxic Battle over the Value of Nuclear Weapons," *European Journal of International Relations* 20, no. 2 (2014): 316–40.
15. Gray, "Nuclear Strategy," 56.
16. Jacob Kipp, "Russian Doctrine on Tactical Nuclear Weapons: Contexts, Prisms, and Connections," in *Tactical Nuclear Weapons and NATO*, eds. Tom Nichols, Douglas Stuart, and Jeffrey McCausland (Carlisle, PA: Strategic Studies Institute, 2012), 131–32.
17. Alexei Fenenko, "The Return of Flexible Response," *Current Digest of the Russian Press* 61, no. 42 (October 19, 2009): 14–15, <https://dlib-eastview-com.proxy1.library.jhu.edu/>.
18. Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave MacMillan, 2003), 243–57.
19. Freedman, 244–45.
20. John G. Hines, Ellis M. Mishulovich, and John F. Shull, *Soviet Intentions 1965–1985*, vol. 1, *An Analytical Comparison of U.S.-Soviet Assessments During the Cold War* (McLean, VA: BDM Federal, Inc., 22 September 1995), 35–47, <http://russianforces.org/>.
21. Herman Kanh, *On Escalation: Metaphors and Scenarios* (New Brunswick: Transaction Publishers, 2012), 290. Originally published in 1965 by Praeger.
22. Andrew J. Bacevich, *The Pentomic Era: The U.S. Army between Korea and Vietnam* (Washington, DC: National Defense University Press, 1986), <http://purl.access.gpo.gov/>.
23. Paul Sonne, "Pentagon Unveils New Nuclear Weapons Strategy, Ending Obama-Era Push to Reduce U.S. Arsenal," *The Washington Post*, 2 February 2018, <https://www.washingtonpost.com/>

24. Robert P. Haffa, "The Future of Conventional Deterrence: Strategies for Great Power Competition," *Strategic Studies Quarterly* 12, no. 4 (2018): 94–115.
25. Haffa, 108–9.
26. Haffa, 98–100.
27. Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 365–67.
28. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton and Company, 2014), 21.
29. Haffa, "Future of Conventional Deterrence," 102–3.
30. Haffa, 109–13.
31. Kenneth Waltz, "Nuclear Myths and Political Realities," *American Political Science Review* 84, no. 3 (September 1990): 731–45.
32. Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs* 70, no. 1 (1990/1991): 23–33.
33. Charles Pierson, "The Atomic Bomb and the First Korean War," *Online Journal of the Strategic Culture Foundation*, 19 September 2017, <https://www.strategic-culture.org/>.
34. Freedman, *Evolution of Nuclear Strategy*, 76–81.
35. Freedman, 73.
36. Fred Kaplan, "Scientists at War," *American Heritage* 34, no. 4 (1983), <https://www.americanheritage.com/>.
37. Bacevich, *The Pentomic Era*, 103–28. The term "pentomic" came from the expansion of the battalion to five companies, again designed for maximum dispersal but able to absorb massive casualties and remain effective.
38. Bacevich, 129–57.
39. Robert Peters, Justin Anderson, and Harrison Menke, "Deterrence in the 21st Century: Integrating Nuclear and Conventional Force," *Strategic Studies Quarterly* 12, no. 4 (2018): 32–36, <https://www.airuniversity.af.edu/>.
40. Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 1–34.
41. Kanh, *On Escalation*, 11, 14.
42. Bernard Brodie, "Nuclear Weapons: Strategic or Tactical," *Foreign Affairs* 32, no. 2 (1954): 217, <https://www.jstor.org/>.
43. Woolf, *Nonstrategic Nuclear Weapons*, 8–9.
44. Robert W. Nelson, "Lowering the Threshold: Nuclear Bunker Busters and Mini-nukes," in *Tactical Nuclear Weapons: Emergent Threats in an Evolving Security Environment*, eds. Brian Alexander and Alistair Millar (Washington, DC: Brassey's, 2003), 68–79.
45. The GBU-57 is the most powerful nonnuclear weapon in the US arsenal. While its full capabilities and yield are classified, it carries 5,300 lbs. of explosives, and according to the *Air Force Times*, the missile can deliver a payload 200 feet into the ground before detonation. The development of a nuclear option has continued as well. Hans Kristensen from the Federation of American Scientists reported in 2016 on a successful test of the B61-12 prototype, which can be configured with yields of 0.3, 1.5, 10, or 50 kilotons. While the depth achieved has not been disclosed, the munition completely buried itself, guaranteeing a ground penetration of at least 3.5 meters. Even at this depth, the ground coupling shock effect is great enough to provide an effect 10 to 20 times more powerful than a surface blast. Given the success of the GBU-57's delivery vehicle at ground penetration, it is reasonable to suspect that this prototype may have traveled much deeper than 3.5 meters.

46. Nelson, "Lowering the Threshold," 76–78.

47. William J. Perry, "The US Does Not Need New Tactical Nukes," *Defense One*, 26 April 2018, <https://www.defenseone.com/>.

48. Kier Lieber and Daryl Press, "The New Era of Counterforce Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (2017): 9–49, doi:10.1162/ISEC\_a\_00273.

49. For the Combined Chiefs of Staff directive issued to Gen Dwight D. Eisenhower on 12 February 1944, see Allied Forces, Supreme Headquarters, Dwight D. Eisenhower, *Report by the Supreme Commander to the Combined Chiefs of Staff on the Operations in Europe of the Allied Expeditionary Force, 6 June 1944 to 8 May 1945* (Washington, DC: Center of Military History, US Army, 1994), v–vi, <https://history.army.mil/>.

50. Schelling, *Arms and Influence*, 1–34.

## BOOK REVIEWS

*Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat* by John P. Carlin with Garrett M. Graff. Public Affairs, 2018, 464 pp.

Recent publication trends involving cyber subjects summarize the past two decades' activity with shaded perspectives about motivation and intent. John Carlin in *Dawn of the Code War*, with Garrett Graff's assistance, covers much-discussed activities from a Department of Justice (DOJ) perspective including Carlin's multiyear role as chief of staff for FBI director Robert Mueller. These depictions offer some expanded views while failing to substantially improve upon similar works including *Rise of the Machines* by Thomas Rid, *Cyberspies* by Gordon Corera, or *Dark Territory* by Fred Kaplan. These other works formulate unique cyberspace perspectives while *Code War* focuses almost exclusively on DOJ dealings with other agencies during and after cyber events. For example, the Qassam Cyber Fighters section merely relates investigatory actions from the Drug Enforcement Administration, FBI, and National Security Agency rather than any efforts or collaboration originating from Carlin. This book is an excellent place to start for those new to the global cyber commons and cyberattacks against the United States, although those with greater familiarity can skip this work.

As mentioned, *Dawn of the Code War* loosely follows John Carlin's exposure as a Justice Department agent and leader for multiple cyber events, including espionage, attack, and influence operations. Each chapter—beginning with his initial 2004 exposure—describes one to two years of an experience between the United States and adversary cyber actors as well as any eventual mitigation. The work explores three primary mitigation policies advanced by the DOJ: demonstrating clearly where US cyberspace laws create boundaries, supporting the US private sector through its actions, and communicating to foreign adversaries that continued espionage and attacks are unacceptable. Every chapter attempts to advocate those tenets to some degree, forging a policy path as well as norm expectations for those unfamiliar with US cyber operations. Each instance reveals individuals Carlin knows and when he worked with them during their time with the Justice Department.

Eight central stories advance as single chapters that begin with China recruiting human intelligence agents to conduct economic espionage through multiyear campaigns based on obtaining corporate positions and physically transferring documents to today's current cyber practices. During his time with Robert Muller, Carlin may have shaped cases like those against GameOver Zeus's criminal activities and China's attacks on the US Office of Personnel Management (OPM), and even exerted some influence investigating Russia's 2016 presidential election interference. Each chapter's single primary case includes subordinate attacks and activities that build an overall picture for the selected time frame. The work addresses how President Bush's cyber initiative could have formed the groundwork to advance cybersecurity before being abandoned by the Obama administration for a fresh cyber start. The Obama administration's reliance on being more naturally tech-savvy than previous regimes probably delayed more stringent cyber approaches against cyber adversaries. Actions against the Iranian Qassam Cyber Fighters' US bank campaign and Russian hacktivist actions in Ukraine took years to pursue and fully develop, and Carlin successfully highlights administrative difficulties in obtaining clear attribution or building any federal consensus about retaliatory actions when pursuing federal criminal cases. Particularly noteworthy are the expanded insights into foreign attacks against US private companies with Iran's destructive Sands Casino attack and North Korea's multiple Sony attacks during 2014.

Each chapter has some additional coverage for recent attacks, with the best overall chapter tying the Target and TJ Maxx credit card attacks to Anthem's data exfiltration before exploring the subsequent larger attacks against the federal government's OPM. The OPM attack describes three separate Chinese-attributed cyberattacks that, in

Director of National Intelligence James Clapper's opinion, impacted central cybersecurity tenets by undermining the confidentiality, availability, and integrity of federal data involved in verifying US federal employees' financial, personal, and security clearance files (361). The three OPM attacks, months apart, each targeted different network systems. OPM's recovery process eventually discovered one piece of installed malware per device, and no attack was discovered until three weeks after the last. Carlin clearly shows that despite the US government's own cybersecurity focus during the relevant time periods, federal agencies failed to meet their own standards for commercial industry. A 90-day cyber-defense improvement sprint in 2015 resulted in only 15 of 29 agencies meeting basic cyber security requirements (365). After 10 years of Carlin's assistance directing policy and legally pursuing adversaries, evidence indicated that barely 50 percent of federal agencies complied with even the most basic preventative measures.

There is some new material about US actions against foreign cyberattacks, but uncovering Carlin's own role was difficult. His appearance seems perfunctory and based on personal connections rather than contributing activity. For example, the Russian-oriented "Slavik" chapter does not include a single action by Carlin. The standard for authors recounting personal actions in their government service—if not a full biography—should be compilations similar to Juan Zarate's *Treasury's War* (2013), describing the Department of Treasury's counterterrorist financial actions. Carlin does possess considerable personal knowledge as a recently departed federal official, though the text fails to convey any sense of urgency or immediacy that he feels toward these struggles from his own experience. The overall conclusion makes a perfunctory mention of a "code war," the need for increased training, and carrying American values onto the Internet—all good ideas but lacking connection to earlier material. Carlin's text offers some learning, but any emphasis on the Justice Department's unique influences unfortunately are absent.

In general, *Dawn of the Code War* provides an adequate introduction to the last decade's cyber activity, especially those in the gray zone of not-war, faced by the United States. Cyberspace novices will get a substantial grounding while more advanced readers may find some interesting nuances about previously studied attacks. Carlin and Graff manage to advance the field somewhat with compiling significant information under a single cover to create a worthwhile stop. The text jumps somewhat chronologically but not to such an extent as to make following the material difficult. Long for an individual account at 400-plus pages, the book reads quickly. I found the material mildly entertaining and beneficial overall. While this work is not my first suggestion to pursue for a cyber history, I recommend that new cyber students add it to their bookshelves and more experienced students consider *Code War* for their backlog. An improvement would be a future work from Carlin depicting his own experiences in greater detail.

Dr. Mark T. Peters II, USAF, Retired

***Nanoweapons: A Growing Threat to Humanity*** by Louis A. Del Monte. Potomac Books, 2017, 244 pp.

When new technologies cross from industry to the battlefield, calls arise to slow the process and consider international implications of using these weapons. Louis A. Del Monte's *Nanoweapons* is one of those calls. A physicist and former executive at IBM and Honeywell, Del Monte led advancements in microelectronics and sensors. His work is a serious attempt to use publicly available information to address the development and use of nanotechnology as weapons. The author brings together ideas normally relegated to science fiction (e.g., laser weapons, artificial intelligence, and self-replicating nanorobots) and uses his technical background to inform the reader as to what is science fact. While his most alarming predictions for humanity's survival project to the year 2050 and



beyond, he argues that his concerns are timely. He indicates that while revolutionary military nanotechnologies (e.g., stealth aircraft) may take decades to field, they are nonetheless currently being developed. Now, according to the author, is the time to discuss the dangers of nanoweapons.

The author's main thesis is that nanoweapons are a danger to humanity that demand greater attention. Despite the secrecy surrounding the development of nanoweapons, Del Monte is confident of their threat. This fear is based in part on the ranking of nanotechnology weapons by the Global Catastrophic Risk Conference at the University of Oxford as the most probable means to cause human extinction by the end of this century. Examples of nanoweapons discussed in the book include nano-enhanced lasers, smaller munitions with increased explosive force, and self-replicating smart nanorobots (SSN). SSNs search for and destroy targets without human input and self-replicate with materials found in the environment. According to the author, SSNs are gravely dangerous nanoweapons that humanity should prohibit. Central to his concern for humanity's survival is what he sees as the inherent difficulty in mounting defenses to nanoweapons given their capability to avoid detection and the ability of those who use these arms to escape attribution. While considerable resources have been dedicated to countering nuclear weapons, little is publicly known about protection from nanoweapons. This is especially concerning to the author because some nanoweapons have characteristics similar to biological pathogens. Giving his readers reason to be apprehensive, Del Monte turns to explaining how today's nanotechnology can be used to create nanoweapons.

While nanotechnology is already improving our computers, sunscreens, and building materials, the first section of the book provides the nontechnical reader an easy-to-understand introduction to nanotechnology and how it may be used in arms development. The author organizes nanoweapons into five categories: offensive strategic, defensive strategic, offensive tactical, defensive tactical, and passive. Examples are provided for each category, along with an explanation of its offensive, defensive, or passive nature. For instance, the offensive strategic category includes artificially intelligent nanorobots that can target particular individuals, hypersonic glide missiles (whose development will rely on developing certain nanomaterials), nano-enhanced fuels, and nonelectric guidance systems. The other categories include additional guidance for organizing nanoweapons. While readers will find these categories helpful, a workable definition of nanoweapons is missing.

With this deep level of organization dedicated to understanding nanoweaponry, the reader would hope for a more useful definition of nanoweapons. *Nanoweapons* are defined in the book's glossary as "any military technology which exploits the use of nanotechnology" (229). Although this definition will capture all nanoweapons, it will also include many items that are not weapons. This definition would include a military finance office using a publicly available desktop computer with a nanomanufactured microchip. Is building a weapon with nanomanufactured components all that is required to make the weapon a nanoweapon? If a dry-docked ship is sprayed with anticorrosive nanocoating—increasing its hull strength tenfold (as an MIT study referenced in the book suggests)—is the ship now a nanoweapon? The book makes clear that nanotechnology is an enabling technology that will empower a wide range of civilian and military applications. But it does not wrestle with the problem that an SSN is fundamentally different than an anticorrosive nanocoating. This issue of defining nanotechnology is a common attribute of nascent scientific fields, but the reader is nevertheless left wanting more. Without addressing this definitional problem directly, Del Monte instead uses other methods to discover what nations are emerging as nanoweapon leaders.

He categorizes the factors needed to facilitate nanoweaponry development and sorts nations by these factors into the Nanoweapons Offensive Capability of Nations (NOCON) list. The most powerful group, nanoweapon nations—such as the United

States and China—has the ability to commercialize nanotechnology, possesses a national desire to strengthen its militaries, and demonstrates an ability to partner with other leading nanotechnology nations. Del Monte goes on to mention other nations on his NOCON list, all of which have varying interactions with nanotechnology. Giving the reader reason to be concerned for the international implications his NOCON suggests, he then highlights the events that may tip us into a nanoweapon-driven war.

He predicts two singularities that will spawn nanoweapon-related international disruptions. In addition to the creation of SSNs, the other singularity is the advent of artificial intelligence (AI) that will exceed human intellect. AI will solve many of humanity's greatest problems, the author posits, but it will also create better SSNs. If AI and SSNs are combined, alliances will form to maintain advantages in a new cold war around the development of AI-powered SSNs. Given their importance, international power will then be rebalanced around nanoweapon capabilities. Nuclear weapon use will increase since nanotechnology will empower their miniaturization and reduce their fallout. It is these disruptions, brought on by the AI and SSN singularities, that Del Monte claims will dramatically increase the chance of human extinction by 2100. Given this pessimistic prediction, *Nanoweapons* next discusses reasons for hope.

The author maintains some optimism for humanity. He notes that humanity has engaged in conflict since the beginning of our existence, but recent developments, such as the Treaty on the Non-Proliferation of Nuclear Weapons and the Biological Weapons Convention, show that humanity can act to prevent its extinction. Once humanity comes to know the existential threat that nanoweapons represent, humanity will act to limit their use and thus avert disaster. What we recognize when we use a new personal computer, he argues, is not the nanotechnology enabling its use but the impressive performance it achieves. The author states that humans understand technology by its function, not the technology itself. Thus, to forestall the need to demonstrate a nanoweapon's threat to humanity, he indicates that current treaties and conventions concerning weapons of mass destruction should also regulate strategic nanoweapons.

A workable and more precise definition of nanoweapons will improve this area of study by allowing policy makers to grapple with nanoweaponry development. It will empower leaders to specifically categorize an adversary's capabilities and document who is developing nanoweapons with greater specificity. Assuming that Del Monte's catastrophic predictions are accurate, more scenarios are needed to better inform technologists, military commands, and national leaders working on ways to prevent the negative implications of these technologies. This work is worth reading because it ties together the technical, political, economic, and practical challenges associated with nanoweapons. The initial portion of the book is especially worthwhile for those seeking an approachable introduction to nanotechnology and its use as weaponry. Suggestions for additional reading in this area of futurism are Peter W. Singer's *Wired for War* and Michio Kaku's *Physics of the Future*. Strategic leaders will appreciate the discussions on organizational problems associated with fielding nanoweapons and rebalancing international power. Tactical leaders will find themselves working through different ways to use and defend against nanoweapons. Finally, fans of science fiction will appreciate a technical introduction to many real concepts previously relegated to fantasy.

Maj Patrick M. Milott, USAF

***Unrivaled: Why America Will Remain the World's Sole Superpower*** by Michael Beckley.  
Cornell University Press, 2018, 248 pp.

Graham Allison's concept of the Thucydides Trap has fed the hubristic notion in polarizing policy debates that China's rise in the world is in relative proportion to America's

decline. While military conflict (economic and trade flaps notwithstanding) may in fact be avoidable as a result of the aggressive and interconnected aspects of other instruments of power, the authenticity of great power competition with China may in fact be just a facade—in every respect of that debate. This view is the overarching thesis of Michael Beckley's new book *Unrivaled: Why America Will Remain the World's Sole Superpower*, originally titled *The Unipolar Era*.

Beckley is an assistant professor of political science at Tufts University and an associate in the International Security Program in the Belfer Center at the Harvard Kennedy School. His work has been featured in numerous popular media (NPR, *Washington Post*, and *Harvard Business Review*, among others). He has served in academia, the think tank community (RAND, Carnegie Endowment) and in government (DOD)—making this book as credible as it is highly readable.

The central thesis of Beckley's argument—that the US will remain the world's *sole* superpower for many decades and perhaps the rest of this century—rests on the supposition that current comparative measures and indices of power do not sufficiently describe, and often fall well short of, articulating relative power. He contends that one of the primary measures, gross domestic product (GDP), exaggerates the wealth and military power of populous countries whose vast output also bears enormous welfare, security, and efficiency costs. Beckley also debunks the supposition that all great powers have predictable life spans (as history demonstrates) by excepting the US due to unique geographic, demographic, and institutional factors combining to keep it in the lead position in perpetuity. These same arguments are also advanced in Peter Zeihan's *The Accidental Superpower* and Tim Marshall's *Prisoners of Geography*.

In chapter 2, Beckley provides a history review, developing his argument via the framework and combined measure, which is quite convincing. He then builds upon this foundation in chapters 3 and 4 to test and make comparisons between the US and its closest and most talked about power rival, China, through a thorough economic and military lens. The primary conclusion economically articulates that the US has much lower welfare and security costs that traditional measures gloss over, creating the impression that China is overtaking the US. However, as Beckley demonstrates, China's economy barely keeps pace as it backs profit-losing companies and tries desperately, but failingly, to fully meet the needs of one-fifth of the earth's population. Likewise, in chapter 4, the results are stark. The US has five to 10 times the military capabilities of China, whose weapon systems are half as capable. Further, China's limited operational experience, training, and lack of combat—coupled with personnel costs 25 percent higher than similar US costs—work against it. Beckley argues that for China to successfully compete in these areas, it must grow much faster than it currently is, which he deems as unlikely.

Chapters 5 and 6 analyze the future prospects of great powers and their implications. In the former, Beckley critiques two theories—balance of power and convergence—in furtherance of his argument in a fair and reasoned manner. In support of the argument, he develops a new framework projecting the rise and fall of nations that draw on separate and credible economic studies underpinned by geography, institutions, and demography. He concludes chapter 5 by noting that the US “has the most potential for future growth, in addition to an enormous economic and military lead,” yet cautions like any astute political scientist that this will not guarantee future unipolarity. Beckley articulates four implications concerning US unipolarity to bolster his thesis and arguments. He advises that a perpetually unipolar US is not assured, yet, if handled properly, can allow the US to prosper indefinitely—another astute argument.

Beckley adeptly cautions that his argument is not about guaranteed perpetual US dominance. For example, the advantages that elevated and have kept the US in its unipolar status could be squandered by restricting high-skill immigration, or allowing special

interests or demagogues to capture political institutions and run the country into the ground. To further balance his argument, Beckley notes that a taming of American power could take several other forms, such as other countries “denying the U.S. access to their domestic markets, suing the U.S. in international courts, bribing American politicians, bankrolling anti-American terrorist groups, hacking U.S. computer networks, and brandishing weapons of mass destruction,” among others. It would take a concerted, concurrent, and persistent effort by a disinterested America to allow this to happen, which is highly unlikely. The supporting chapters clarify these counterarguments while also reinforcing his thesis.

To make his case, Beckley sets about developing his own framework for measuring power and assessing trends. He then builds another framework for predicting power trends, subsequently using it to “assess the future prospects of today’s great powers.” Lastly, he cogently ties the two together and discusses the implications of his findings on world politics and US policy. As noted earlier, measures such as GDP and the Composite Indicator of National Capability (CINC) (an index combining military spending with data on troops, population, and industrial output) alone do not aggregate and illustrate the true picture of power according to Beckley. He explains how he takes the advice of historian Paul Bairoch by “simply multiplying GDP by GDP per capita, creating an index that gives equal weight to a nation’s gross output and its output per person” to derive a more accurate measure of power.

For those interested in political science and/or foreign or international affairs, Beckley’s arguments will provide a new and refreshing look updating tired, older theses. At 248 pages, his book can easily be read over a weekend.

Brig Gen Chad Manske, USAF  
Commandant, National War College

***Cyber Security: Threats and Responses for Government and Business*** by Jack Caravelli and Nigel Jones. Praeger Security International, 2019, 245 pp.

Finding the right vector to begin any comprehensive cybersecurity practices and policy discussion can seem an Augean task. Jack Caravelli and Nigel Jones make significant headway toward those ends as *Cyber Security: Threats and Responses for Government and Business* excellently captures high-level aspects likely to influence the next 10 to 20 years of cybersecurity implementations. The technical descriptions run a little light, although the overall text handily summarizes difficult topics into useful references for those wanting to increase their own background knowledge. Chapters by the individual authors comprise about half the book, with two chapters written as combined works. Further, the text recaptures a previously published Information Assurance Advisory Council report discussing the expanding Internet of Things (IoT) implications. *Cyber Security* is a well-referenced, effectively sourced text that also includes many useful diagrams. It is targeted toward mid-level cyber policy professionals looking to grow their overall knowledge base.

One gap, common with similar coauthored works, is the lack of any unifying theme or thesis beyond the central cybersecurity theme. Frequent mentions occur of a chapter’s place as part of the larger text, but each chapter stands independently. Caravelli tackles the international relations piece through a first section focusing on terrorism, crime, and espionage topics. The two authors together then explore a single chapter on advanced technical topics including quantum computing, artificial intelligence, and big data. Finally, Jones brings in several case study chapters examining how states use innovation and what policies currently exist and summarizing changes in United Kingdom cyber strategy over the past 10 years. As a rough outline, the first section comprises three chapters con-

centrating on offensive cyber usage, the middle section discusses technological innovation over four chapters, and the final section's three chapters explore state-based policy response to the aforementioned changes.

Evaluating recent cybercriminal and terrorist high-level impacts serves only to repeat areas already explored in other material for the well-read expert. However, as a basic cybersecurity approach, describing foundations from the historical perspective serves as a solid practice. Some of the best parts of the book surround the detailed descriptions of the Islamic State of Iraq and Syria's (ISIS) cyber-associated Middle East terrorism and the Obama administration's challenges dealing with Chinese intellectual property theft. When recounting geopolitical issues, Caravelli extensively discusses challenging relations between Russia and the United States over the past 10 years, including the 2016 election controversy. He also strikes a home run with his inclusion of a full callout box discussing Gen Valery Gerasimov's policies on information war and full-spectrum conflict. Russia's chief of the General Staff is considered the father of Russian nonlinear doctrine. The section adequately covers most recent highlights—with the noted excellent exceptions—while avoiding overly technical details.

The second section includes more technical detail about upcoming innovative changes while remaining focused on the policy perspective. As mentioned, the two authors reframe an IoT report before using their own research to study quantum computing, big data, and artificial intelligence. The section considers what cyber solutions may appear through these innovations. One must wonder why the IoT piece's report format was chosen as the material clearly is visually and stylistically different from the remainder of the book. The report emphasizes policy aspects for mitigating IoT threats without ever really discussing the independent technological challenges. The author's recommendations for overall solutions again roll out suggestions for resilient systems, security from the start, and partnerships but also advocate clearly unwieldy decisions such as returning to paper ballots across the US rather than risk hack-prone voting machines (154).

The third section mirrors the first while considering events from a state perspective rather than from each individual attack. When discussing innovation practices, Jones uniquely uses an *SC Magazine*-based award program to highlight a security practice migration from hardware to software and app-based practices. Later, the chapter steps back from evaluating innovative cyber practices to providing solutions that encourage innovation in any company or organization. The final two chapters have national case studies summarizing how various nations and regions—including the US, China, Russia, NATO, and the Gulf Cooperation Council—have dealt with cyber. Although the studies are expertly presented and contain useful information, they remain somewhat disconnected in execution from the earlier topics.

References abound throughout the work to uncover new material discussing cybersecurity, but one of the more frustrating points deals with no items being sourced through either endnotes or footnotes. Some of the discussed items are either controversial or so intriguing one would like to examine the original source material. For example, the text claims that the average starting salary for an information technology worker in the United States is \$116,000 a year; however, a quick Google search suggests \$55,000–\$66,000 a year—less than half of the claimed amount. Also, the innovation chapter could have been expanded and better explained at some points. It implies that merely using cyber qualifies as innovation and then seeks further innovation types inside those models. Each referenced area is split into cyber innovation types—including vulnerability management and firewall implementation—rather than focusing on an innovation's business value, such as improved security, faster deployment, or coordinated value streams. The cybersecurity practice known as DevSecOps (development, security, and operations) incorporates technology from initial development to final delivery and has proved a profitable business area.

Caravelli and Jones likely missed a critical discussion area through not evaluating how improved cyber practices benefit more than just basic cybersecurity outcomes.

Overall, *Cyber Security* strikes all the required notes for an introductory volume in this genre. The comprehensive collection reads easily, covers all the basic areas, and suggests multiple locations for more advanced research. For those approaching this work from any policy standpoint, the text provides an exceptional introduction. As a minor complaint, while the threats and historical responses get detailed coverage, I was looking forward to more discussion about future potential actions as suggested by the two experienced authors. While not sufficiently structured to make a useful desk reference, the book could work as core material for a larger cybersecurity course or for those looking to expand their own knowledge. For the most part, those pursuing cybersecurity policy issues for either business or government purposes should find this a useful addition to their own library.

Dr. Mark T. Peters II, USAF, Retired

*Army of None: Autonomous Weapons and the Future of War* by Paul Scharre. W. W. Norton & Company, 2018, 446 pp.

*Army of None* sets out to explore the following questions: Given rapid advancement in artificial intelligence (AI) technology, should robots be allowed to make life-or-death decisions? To what degree should humans be involved in the decision-making process? Should we, or could we, ban autonomous weapons? Author Paul Scharre is a former US Army Ranger and currently the director of the Technology and National Security Program at the Center for a New American Security. While working for the Office of the Secretary of Defense from 2008 to 2013, he directly influenced US defense policy on autonomous weapons by leading the DOD working group that drafted DOD Directive 3000.09, *Autonomy in Weapon Systems*.

Scharre's apparent goal in writing *Army of None* is to open a dialogue on the use of autonomous weapons. To begin an informed conversation, however, he must first define "autonomy," which is more troublesome than it appears. The differences between automatic, automated, and autonomous systems are obscure and difficult for even experts to understand, but Scharre gives tangible examples from his time as a Ranger in Iraq and Afghanistan that make the tricky distinctions clear to the layman reader. Scharre also aids the reader by boiling down complicated explanations into simple pictures before he moves on to the next topic, enabling even the most inexperienced reader to grasp concepts like supervised autonomous weapons systems.

To continue building the reader's mental model of autonomous weapons, Scharre points out that the idea of such weapons is not new. The German G7e/T4 Falcon torpedo saw combat in 1943, and it used a passive acoustic homing seeker to hunt down its prey. Over the next several decades, countries around the world would develop increasingly more capable weapons, resulting in many of the weapon systems we use today. Scharre dedicates several chapters to portraying the land-based Patriot missile system and the ship-based Aegis combat system. He interviews subject matter experts in the DOD and outlines the capabilities and risks that each system brings to the fight. Careful to avoid bias, Scharre balances praising the effectiveness of the autonomy to engage targets with real-world examples of fratricide and opens discussion on best practices when using such powerful autonomous weapons.

After defining autonomy and giving a brief background on its past and current use in war fighting, Scharre devotes the majority of the book to seeking answers for whether or not we should entrust life-or-death decisions to machines and to what degree. He does this by interviewing a diverse selection of industry experts and offering their views and perceived courses of action, allowing readers to form their own opinions on the subject.

Those interviewed range from former US deputy secretary of defense Bob Work, to program managers at the Defense Advanced Research Projects Agency (DARPA), to private companies developing commercial applications of AI. To further encourage self-reflection in the reader, Scharre refrains from stating his personal stance until the conclusion, and even then he admits that there is no black-and-white answer. Instead, he concludes that “states must come together to develop an understanding of which uses of autonomy are appropriate and which go too far and surrender human judgment where it is needed in war.”

While many fundamentals of war fighting are timeless, the technology we use to fight is ever evolving. A shift in focus toward peer-to-peer conflict forces our Department of Defense to address the hairy questions Scharre asks. Whether artificial intelligence will be used on the battlefield is not the question to be asking. Rather, our decision makers must continue to ask how autonomous weapons will be used in future conflict without compromising the moral high ground the world expects the American military to hold. *Army of None* is a must-read for all who find themselves working with or around autonomous systems. It is better for us as a nation to debate the potential uses of autonomous weapons now in peacetime instead of leaving ourselves to make quick decisions during the next conflict.

1st Lt Nathaniel Lewis, USAF

***On the Brink: Trump, Kim, and the Threat of Nuclear War*** by Van Jackson. Cambridge University Press, 2019, 236 pp.

*On the Brink* covers very recent current events from the author’s perspective and speaks to being on the precipice of nuclear war. In this context, it is vital to know the culture and history of the major players. An expert in this field and a known Korean security expert, Van Jackson served in the Obama administration. He describes his research as broadly concerning the intersection of Asian security and US strategic thought. His blend of academics and practical experience infuses his US foreign policy analysis.

The book documents the politics between North Korea and the United States. They are illustrative of a potential path toward nuclear war, but there are many assumptions about how both countries will react. Nuclear war would be horrific, and rational people may threaten it with no intention of following through on that threat in order to meet some of their policy objectives. The bluff factor has always been part of North Korea’s politics, with relatively minor skirmishes executed in an effort to show its resolve.

Although the Korean peninsula is the book’s focus, its lessons apply universally. The author provides an outstanding narrative of recent events surrounding the North Korean crisis. Countries have distinctive cultures and thus react differently to threats, whether real or bluster. Jackson reemphasizes the need to always consider the consequences of actions and words. In this case, if the Trump administration did not push back against North Korea, would the regime have continued its behavior and pursuit of nuclear weapons? Which scenario is more susceptible to a nuclear war: US capitulation to any threat levied or tough diplomacy? The current approach is not traditional, but past approaches have repeatedly proved ineffective.

The Nuclear Nonproliferation Treaty in the early 1990s started us on this journey when President Clinton’s administration pressured North Korea. In 1994 Jimmy Carter intervened to de-escalate tensions between the two countries. The author works through the historical aspects since that time and details how the North Koreans reacted to various administrations.

One item to consider for North Korea is that it never truly deviated from the goal of obtaining nuclear weapons and simply used any available means to get them. It seems to

have a fascination with becoming a nuclear-armed state and a power to be reckoned with. Negotiations have always tried to stop proliferation but have failed in this regard since they rarely considered what the North truly wants. However, by always giving in to demands, the United States demonstrated that it would act tough but not follow through in an effort to eliminate the threat and maintain the peace in the long term.

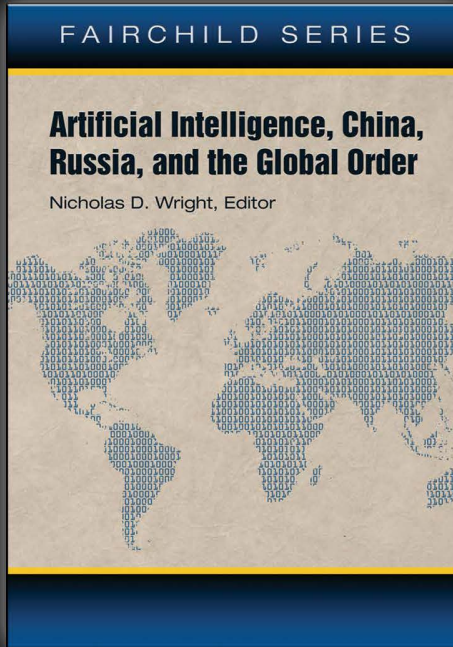
The implication of books like this is that we can pick and choose how alternative events could have unfolded if elections went differently—if only a tweet wasn't sent or a different dialogue was pursued. In diplomacy, the actions tend to be slower and more measured. The difference now is that a nonpolitician businessman is in charge—one used to making rapid decisions. So it seems natural that the normal political apparatus would be alarmed. The question is whether normal politics were working and should have continued to set the foreign policy goals and actions. The nuclear testing program by North Korea proved the fallibility of previous sanctions and policies from prior administrations. If we believe that coarse language could start a nuclear war, then we must think that the recipient is potentially unstable and given to hasty decisions. If the adversarial political leadership is unstable, is it likely that it would start a war with no rational basis anyway? With North Korea labeled as paranoid in some circles, do we need to tread lightly to prevent incidents? Or is a firm hand needed in both dialogue and a willingness to back up rhetoric?

Throughout the Obama administration, the stage was set to continue working toward nonproliferation or to take a different approach. Obama chose the former. It is not clear what policy President Trump should have followed, but it seems clear that previous administrations were unsuccessful in their approaches. Although many scholars may not agree with Jackson's conclusions, there is no doubt he is well versed in the activities on the Korean peninsula. He has written a thought-provoking book for anyone concerned about global politics.

**CMSgt Frank Murphy, USAF, Retired**



## Our Latest Publication



### **Artificial Intelligence, China, Russia, and the Global Order**

A wide variety of perspectives on the different uses of artificial intelligence (AI) in Russia and China and the impact this will have on the global order. Essays are from leading defense professionals, academics, think tanks, and policy developers. A comprehensive primer for those concerned with how emerging technologies will influence the West's near-peer competitors.



**AUP**  
AIR UNIVERSITY PRESS

<https://www.airuniversity.af.edu/AUPress/>



IN MEMORIAM  
**DAVID R. METS**  
1928–2019



We pay tribute to author, scholar, and warrior Dr. David R. Mets, lieutenant colonel, USAF, retired. Between 1965 and 2013, Dr. Mets produced over 80 print and e-books, papers, articles, and book reviews—the majority with Air University Press. His works cover such topics as airpower, technology, NATO, and military leaders, spanning the early twentieth century until today (see <https://www.airuniversity.af.edu/AUPress/> and <https://www.worldcat.org/>). He graduated from the US Naval Academy and was commissioned a US Air Force officer, eventually flying the B-25 and C-130 gunship. Dr. Mets earned a PhD in history from the University of Denver, co-founded the Air University School of Advanced Air and Space Studies (SAASS), and served as a professor for the first 13 graduating classes. He will be remembered fondly by Air University faculty, friends, colleagues, and students and sorely missed by Air University Press. We salute Dr. Mets for his innovation and contribution to the study and discussion of airpower and the legacy he leaves to the Department of Defense and the Airmen of today and tomorrow.

### **Mission Statement**

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

### **Disclaimer**

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

### **Comments**

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

### **Article Submission**

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

**[StrategicStudiesQuarterly@us.af.mil](mailto:StrategicStudiesQuarterly@us.af.mil)**

**Strategic Studies Quarterly (SSQ)**

600 Chennault Circle, Building 1405

Maxwell AFB, AL 36112-6026

**Tel (334) 953-7311**

View and Subscribe to *Strategic Studies Quarterly* at

**<https://www.airuniversity.af.edu/SSQ/>**

### **Free Electronic Subscription**

Like SSQ on Facebook at **<https://www.facebook.com/StrategicStudiesQuarterly>**

*Strategic Studies Quarterly* (SSQ) (ISSN 1936-1815) is published by Air University Press, Maxwell AFB, AL. This document and trademark(s) contained herein are protected by law and provided for noncommercial use only. Reproduction and printing are subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the SSQ editor for assistance.