★★★ Department of the Air Force ★★★

Æther

A Journal of Strategic Airpower & Spacepower

Senior Leader Perspective

Air Superiority
General James B. Hecker, US Air Force

Managing Risk

Mineral Supply Chains and Space Assets
Gregory Wischer
Gregory Autry
Morgan D. Bazilian

Technology, Society, and War

Emerging Laws and Norms for AI Facial Recognition Technology
Alison Lawlor Russell

Energy Web Dominance
Paul Calhoun

Cyber Red Lines
Denise L. Tennant
Louis Nolan
Deanna House

Elements of Deterrence

Effective Assurance
Luke R. Stover

Tensions on the Peninsula
Jessica Reneé Taylor

Transforming a Bureaucracy

Policy Change Takes Flight
Kelly Atkinson

Vol. 3 No. 2 ★ Summer 2024

ÆTHER

A Journal of Strategic Airpower & Spacepower

https://www.af.mil/

https://www.spaceforce.mil/

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

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

ÆTHER

A Journal of Strategic Airpower & Spacepower

SUMMER 2024 VOL. 3, NO. 2

3 Letter from the Editor

Senior Leader Perspective

5 Air Superiority
A Renewed Vision
General James B. Hecker, US Air Force

Managing Risk

12 Mineral Supply Chains and Space Assets
Mitigating Manufacturing Dependencies
Gregory Wischer
Gregory Autry
Morgan D. Bazilian

Technology, Society, and War

26 Emerging Laws and Norms for AI Facial Recognition Technology
Alison Lawlor Russell

44 Energy Web Dominance
A Proposal for a Fourth Offset Strategy
Paul Calhoun

60 Cyber Red Lines
Government Responses to Cyberattacks on Critical Infrastructure
Denise L. Tennant
Louis Nolan
Deanna House

Elements of Deterrence

73 Effective Assurance
A Strategic Imperative
Luke R. Stover

85 Tensions on the Peninsula
Strategic Communication for the US-Northeast Asia Alliance System
Jessica Reneé Taylor

Transforming a Bureaucracy

99 Policy Change Takes Flight
The Department of the Air Force Women's Initiatives Team
Kelly Atkinson

FROM THE EDITOR

Dear Reader,

The many facets of US global leadership require continual refining as America adjusts to the realities of persistent geopolitical, market, and technological uncertainty. Whether these updates take the form of laws protecting privacy or critical supply chains or result in policies that clarify red lines and strategic messaging, decisionmakers must respond and adapt in order to preserve US leadership in the world. At the organizational level, innovative advances in all-domain warfare and new ways of analyzing the human domain demand similar honing of technology and processes. And none of this occurs in a vacuum. America's ability to lead with strength, advocate for peace and justice, and oppose tyranny and violence depends in full on our global network of strong Allies and partners.

In the spirit of alliances, we are extremely honored and grateful to present a **Senior Leader Perspective** by US Air Force General James B. Hecker, Commander of US Air Forces in Europe, US Air Forces Africa, and Allied Air Command, and the Director of the Joint Air Power Competence Centre, a NATO Center of Excellence. General Hecker calls for the United States and its Allies and partners to adapt to dispersed operations of forces and headquarters, reconceptualize risk delegation and decision authority, and innovate with the right mix of low-end and high-end capabilities.

In **Managing Risk**, Gregory Wischer, Gregory Autry, and Morgan Bazilian discuss the mineral-intensive composition of major space assets—satellites, direct-ascent antisatellite weapons, and rocket bodies—to highlight supply-chain vulnerabilities. Three key policies will mitigate risk and the resulting national security vulnerabilities.

In our second forum, **Technology, Society, and War**, Alison Russell presents findings from a global study on public- and private-sector facial recognition technology across 20 countries and the EU. In the face of either a total lack of rules and regulations or laws that do not protect citizens from their governments, the United States and its Allies and partners should establish and promote norms that safeguard human rights. Paul Calhoun presents DARPA's innovative energy web dominance framework. This framework will provide new and more resilient methods to achieve military effects, principally in the delivery of energy, through breakthroughs in wireless energy distribution.

The last article in the forum, by Denise Tennant, Louis Nolan, and Deanna House, calls for the establishment of policy red lines in the realm of adversary cyber operations. Such red lines will also help define what constitutes cyber operations in the gray zone.

In **Elements of Deterrence**, Luke Stover examines the concept of assurance, and advocates for a clear delineation between assurance and deterrence. In today's world, alliances and partnerships provide asymmetric advantages, as they are grounded in a firm commitment to the multiple facets of assurance. The forum concludes with an article by Jessica Taylor, who cautions about the strategic messaging the US-Northeast Asia alliance system sends to Pyongyang through its responses to North Korea provocations and alliance system exercises. Avoiding deadly miscalculations on all sides requires clear communication and long-term policy stability on the part of the member nations of the alliance system.

Our final forum, **Transforming Bureaucracy**, considers institutional policy change. Kelly Atkinson analyzes her decade of work with the Air Force Women's Initiatives Team through a new framework of organizational theory that builds upon rational actor theory and addresses the challenges of collective action, emphasizing the roles played by change agents, power brokers, and the frozen middle.

Thank you, as always, for your support of the journal. Team *Æther* wishes you a good second half of 2024. Æ

~ The Editor

AIR SUPERIORITY

A Renewed Vision

General James B. Hecker, US Air Force

The rapid expansion of small unmanned aerial systems in the battlespace, as evidenced in Russia's war in Ukraine, upends our traditional definition of air superiority. In a near-peer conflict, adversaries' advanced systems would likely render untenable the US Air Force's unblemished 70-year record of air superiority against crewed threats. In response, America and its Allies and partners must adapt and innovate, culturally and in how we organize, train, and equip our forces and in how we plan, execute, and command and control operations. Necessary adaptations include dispersed operations of both forces and headquarters and a reconception of delegating risk and decision authority. A balanced mix of high- and low-end capabilities is achievable if we are innovative at both the system and organizational levels.

April 15, 1953. An unremarkable day in the news, but one with enduring significance for modern airpower practitioners. The date marks the last occasion when US forces suffered fatalities from a manned aerial attack—in this case a 1920s-era Polikarpov Po-2 on a nighttime harassment mission in the waning months of the Korean War. The watershed event quietly became the opening bookend of the US air superiority era, and although there has never been a guarantee of air superiority, the United States and its Allies have increasingly treated it as an article of faith ever since.

The US Air Force quite rightly takes great pride and inspiration in this 70-plus-year air superiority track record. But a wise airpower practitioner knows the relatively permissive air environment encountered over the last 30-plus years in Operations Inherent Resolve and Enduring Freedom is not indicative of current and future conflicts. Indeed, the rapid expansion of small unmanned aerial systems (sUAS) on display in Ukraine portends a complicated and deadly air-to-surface threat in any future war and challenges the utility of benchmarking the air superiority definition as defense against manned attacks. Furthermore, any conflict with a near-peer adversary will include both surface-to-air and air-to-air threats of such mass and capability that assuming our perfect 70-year track record of gaining and maintaining total air superiority would be irresponsible, if not dangerous.

General James B. Hecker is the Commander, US Air Forces in Europe; Commander, US Air Forces Africa; Commander, Allied Air Command; and Director, Joint Air Power Competence Centre.

With this context in mind, a few questions remain: What event will provide the closing bookend to this exceptional era, how can the United States and its Allies ensure continued dominance in the air domain, and what should NATO nations do about this shifting paradigm?

To that end, I thank *Æther* for the opportunity to address these issues. Considering all the changes in the operational and strategic picture, we must take a holistic approach to create a renewed vision for the air domain. This short article will emphasize doctrinal, materiel, and information-sharing aspects as the lens through which we can both make sense of the new and emerging operational environment and think deliberately about what the broader Western airpower community can do to mitigate the associated risks and maximize our strategic potential. NATO nations can take powerful lessons from Ukraine, as exemplified by its development and use of the low-cost/high-yield Sky Fortress air defense program. We can also learn and implement capabilities and capacity from NATO's newest members: Finland and Sweden.

Air-Land Integration

A major challenge NATO faces is increasingly congested and contested airspace, both by adversary threats and by the services' competing tactical priorities. Doctrine gives one mechanism to address this challenge. Battle management areas are already in US Joint doctrine, but there are still issues to be resolved during implementation that must be tailored to each situation. At a recent conference sponsored by the Joint Air Power Competence Centre (JAPCC) and hosted at NATO Air Command (AIRCOM), air-land integration was one of the primary topics. All participants gained a new understanding of the battle management area topic, and the Air-Land Integration syndicate identified follow-up areas for both AIRCOM and US Air Forces in Europe (USAFE) staffs.

Russia's war in Ukraine reaffirms that air superiority remains job number one. But we must be clear about our purpose. The air component does not simply pursue air superiority for its own sake. Air superiority is not just the first thing we work toward; it will typically remain our top priority—even if it becomes a low weight-of-effort later in the campaign—because it grants us freedom of maneuver to accomplish all other tasks and because attrition rates would otherwise become prohibitive. We have known this since the combined bomber offensive of World War II, and the current situation in Ukraine is a constant reminder of the terrible cost of a stalemate in the air.

Battle management areas are rightly intended to increase flexibility and independent action, but we must also ensure any changes do not impinge on the air component's freedom of action or negatively impact our support to the terrestrial domains. Just what are combined forces air component commander assets doing in the higher strata? A great proportion of those sorties are delivering close air support and battlefield air interdiction fires through the lower strata directly in support of the ground commander and Joint Force commander objectives.

This does not mean that the lower tier of the airspace is the US Air Force's by birthright, but rather that the principle of "ability to command and control" should be applied. Today's Airmen have always been and will remain keenly focused on the vertical dimension. The

72-hour targeting cycle, though it has room for improvement, is the mechanism by which the air component produces predictable and sustainable airpower from the entire Alliance. Ample flexibility remains to meet the ground commanders' needs with pre-allocated on-call close air support and interdiction missions, but we are likewise committed to finding innovative ways to improve the responsiveness of airpower.

I am encouraged that *Æther* is following up with this difficult topic in its next issue and encourage all participants to bring a multidomain operations perspective to the conversation. Toward that end, all participants in this debate need to find ways to think less from parochial service perspectives and more with an ecumenical lens to match the best asset to the desired effect across the entire battlespace. This is a daunting task and my challenge to all involved.

Ukraine Lessons

There are abundant lessons from Russia's war in Ukraine, of which a few highlights are addressed here. For a more detailed assessment, please reference the recently published article in issue 37 of the *Journal of the JAPCC*, which summarizes the unclassified conclusions from our ongoing study of the war in Ukraine.[1]

Deterrence by Denial

First, deterrence by denial depends upon having the right forces—equipped, trained, and proficient—that can win. In other words, when asking what force posture provides a credible deterrent, the answer is to be able to readily demonstrate that NATO possesses the forces it would take to forcibly deny the adversary their objectives. Authoritarian regimes are not likely to be constrained by public disapproval of military adventurism, so we must appeal to their rational interest that conflict with NATO is not worth the cost and risk to their national forces or regime.

Balanced Effort

Second, we can derive many lessons from the relative stalemate in Ukraine. NATO nations cannot count on high-end capabilities alone to win the fight, as the proliferation of low-cost threats makes engagement with high-end weapon systems unsustainable. In addition to grossly underestimating Ukraine's political, military, and social resolve, Russia also expended the lion's share of its precision munitions in the early phases of the war to little effect, though it is reconstituting those munitions at pace. Without a campaign plan, robust targeting process, and sufficient electronic warfare resources, Russia initially squandered its precious stock of precision munitions, which it is now frantically trying to replenish.

1. Joe Goodwin, "Allied Air Command Lessons from Ukraine: Implications from NATO Air & Space Power Conference," *Journal of the JAPCC* 37 (May 2024), https://www.japcc.org/.

Mass and Scale

Third, and an important distinction from the second, is the age-old principle of mass. In the industrial-scale warfare, any war between large combatants that is not decided in its early campaigns will devolve into an industrial war of attrition. Short, decisive campaigns such as the Gulf War are, in fact, the exception that proves the rule. Ukraine is the norm.

Economics, Technology, and Society

Fourth, the reality of industrial war leads to additional conclusions, namely, winning such a war depends on overall economic strength and resiliency, the ability to adapt and innovate, and the strength of political will and social cohesion. Our Alliance has tangible strengths in this area: A diverse and overlapping set of capabilities from various national defense industries is a strategic strength—as long as our Allies and partners have taken an integration-by-design approach from the beginning to achieve day-zero interoperability. In full-scale conflict, Alliance members would likely quickly overcome challenges, such as the glacial pace of procurement processes and policy roadblocks to interoperability and information sharing, especially if NATO were under attack. We must address those issues with the same vigor now to create the day-zero capabilities we need to deter and defend in the future.

A Strong Focus on Adaptability and Innovation

Sky Fortress

Notwithstanding these general observations, Ukraine's adaptability and innovation deserve special attention. From the early days of the war, Ukraine has been highly innovative at adapting sUAS for anti-armor, antipersonnel, interdiction, reconnaissance, and artillery-spotting missions. Once Russia belatedly began competing in this space, Ukraine adapted again, developing the wildly imaginative Sky Fortress system—an acoustic passive-detection system that has proven highly effective at identifying incoming Russian aerial attacks, particularly drones.

Sky Fortress was the brainchild of a handful of Ukrainian scientists who mounted elevated microphones all around the country and connected them with cellular and radio networks. Using advanced computing to process the results, Sky Fortress quickly identifies and locates incoming attacks and triangulates their likely destinations and flight paths. This information is relayed to mobile firing groups (MFGs) equipped with truck-mounted machine guns and man-portable air defense systems (MANPADS). The MFGs then maneuver to the expected engagement point and use optical, thermal, and radar-guided tracking systems to complete the engagement. Ultimately, low-cost engagements of low-cost systems bring the fight back to the right side of the cost curve.

Notably, Sky Fortress also has exemplified many tasks most appropriate for machine learning and artificial intelligence (AI/ML). Ideal tasks for AI/ML are clearly defined, with large datasets upon which detailed analyses and correlation must take

place in near-real time. For such tasks, human judgment is generally not required until a decision must be made based on that data and analyses. We should continue to look for modest, rapidly attainable opportunities for automation that empower human decisionmakers and accelerate decision cycles.

Exchange Cost and Sustainability

Applying the lesson of Ukraine's adaptability and innovation to the challenges of maintaining the air superiority era puts a spotlight on NATO's approach to air defense. NATO air defense systems such as Patriot are highly effective, and Ukraine's ability to fuse so many systems into a coherent defense has been impressive, but when Ukraine utilizes a million-dollar missile to shoot down a Shahed drone that costs perhaps $20,000, it ends up on the wrong side of sustainability, mass, and the cost curve.

Yet, this threat-versus-defender cost comparison only tells part of the story. Other factors must be considered: What is the value of the defended asset? If a high-end system is expended to defend a high-value defended asset, then perhaps the exchange was strategically worth the difference in cost: the value of the defended asset far exceeds the cost of the interceptor. Further, we must consider any secondary effects. Perhaps the high-end system is defending a nuclear power plant. Not only is that plant of great value—in terms of power production and replacement costs—but also the secondary effects of a radiological event would be catastrophic. From that perspective, expending the high-end system, even against low-cost threats, is an outright bargain.

This more accurate understanding on the cost of action versus inaction exemplifies the need for a balanced mix of high- and low-end capabilities. Such a high-low mix ensures we have the top capabilities to execute our most challenging missions while still affording the overall mass (both force structure and equipment) to cover all geographic responsibilities and provide enough depth to sustain ongoing operations and remain resilient to losses. Ukraine is leading the way with Sky Fortress. With its truck-mounted antiaircraft artillery systems, its MFGs accomplish most engagements with bullets for pennies on the dollar compared to the cost of the drone, not to mention the value of the defended asset.

A Stronger NATO

The recent accession of Finland and Sweden to NATO punctuates another significant anniversary—75 years of the most successful defensive alliance in history. These two new Allies make our deterrence posture even more credible by securing the perimeter of the Baltic Sea region, expanding the Alliance's reach and expertise in the Arctic, and extending NATO's border with Russia by 1,300 kilometers. Inspired by Russian President Vladimir Putin's illegal war of aggression, the Alliance is reinvigorated and more robust than ever.

Operationally, our new Allies bring great proficiency in combined operations. The transparency and interoperability demonstrated by the Nordic Defense Cooperation are the example to which the rest of NATO should aspire. Additionally, both nations are world-class practitioners of dispersed operations. Agile combat employment (ACE) is a

bit of a "back to the future" development for many in NATO—it was part of our planning and training during the Cold War, but we let that competency atrophy over the last 30 years. In contrast, our new Nordic Allies, necessitated by their former policies of nonalignment, sustained this capability.

Maintaining this combat edge is more than just practice. Sweden's Gripen, for example, can be combat turned for an air-to-air mission from a highway strip by a sergeant and a handful of conscripts in about 15 minutes. Practice is a big part, but it is only possible because of a host of conscious design decisions, capable Airmen trained to accomplish multiple tasks, judicious delegation of authority and risk, and a nonpunitive command culture. As US and NATO forces move boldly toward ACE operations, this is just one area among others where we can learn from our new Nordic Allies.

NATO brings together 32 nations with widely varied sizes, economies, and militaries, not to mention geopolitical challenges. Even still, NATO nations are united in our broadest values and steadfast commitment to collaborative defense. While the variation in available means can create some challenges to fielding a cohesive fighting force, the lessons and observations above lead to some exciting conclusions, such as the potential for specialization. As an example, it is not practical or even necessary for all NATO members to field a fifth-generation air force, nor do any of us have the resources to excel at everything. If, instead, nations specialize to deliver elements of the high-low mix, we can field a force with the depth and mass to credibly deter and, if necessary, defeat the diverse threats of near-peer adversaries.

Sky Fortress's relevance to NATO and our national processes could not be clearer. Of course, technological development is dynamic and unpredictable; the combatants and other nations will continue to adapt. The point is not that Ukraine's solution today will be 100 percent of our solution tomorrow or that other systems or companies could not be used for the same task. Rather, Sky Fortress simply exemplifies the importance of innovation, adaptability, procurement processes, cost, mass, interoperability, and more. Across the military, industry, and academia, the United States and its Ally and partner nations need to ask if they are aspiring toward the Ukraine model, or if they are complacent in traditional ways of doing business.

Conclusion

USAFE and AIRCOM will continue to update the lessons learned from Ukraine, but the key points discussed herein are unlikely to change, as is the imperative for action. All Airmen have a key role in making sure NATO is a ready, resilient, and adaptable force. Through readiness and our defensive alliances, we will be an effective deterrent by being prepared to prevail. Æ

MINERAL SUPPLY CHAINS AND SPACE ASSETS

Mitigating Manufacturing Dependencies

Gregory Wischer
Gregory Autry
Morgan D. Bazilian

Space is an increasingly competitive military domain. Both the United States and China seek to build and deploy significant numbers of space assets, most of which are mineral-intensive. The mineral compositions of three important space assets—satellites, direct-ascent antisatellite weapons, and rocket bodies—require the United States to import minerals, particularly from China, for their construction. Consequently, the US space industry, and thus the US government, faces the associated risks of supply chain disruptions that can restrict mineral availability and cause price volatility, negatively impacting space asset production. This article proposes three policies to mitigate such risks to the mineral supply chains.

Space is an increasingly important—and contested—military domain.[1] Most of the growing number of space assets being built and deployed by the United States and China are mineral-intensive. Yet US supply chains for space assets depend heavily on mineral imports, often from China. Mechanisms such as foreign export controls can restrict mineral availability and cause price volatility, thus negatively impacting US manufacturing of space assets.

To mitigate import disruption risks to the supply chains of these assets, the US government—with the US Space Force as the primary coordinator—should adopt the following policies: stockpile minerals vital to US space assets, similar to the Strategic Petroleum Reserve or the National Defense Stockpile; provide concessional financing for US space companies to sign long-term, fixed-price mineral offtake agreements;

Gregory Wischer, founder and principal of Dei Gratia Minerals, holds a master in security studies from Georgetown University.

Dr. Gregory Autry, director of space leadership, policy, and business at the Thunderbird School of Global Management and professor at Arizona State University, is the author of A New Entrepreneurial Dynamic *(Flat World, 2022).*

Dr. Morgan Bazilian, director of the Payne Institute for Public Policy and professor of public policy at the Colorado School of Mines, is the author of Analytical Methods for Energy Diversity and Security: Portfolio Optimization in the Energy Sector *(Elsevier Science, 2008).*

1. Elbridge Colby, *From Sanctuary to Battlefield: A Framework for a US Defense and Deterrence Strategy for Space* (Washington, DC: Center for New American Security, January 2016), https://www.cnas.org/.

and impose environmental and labor (E&L) tariffs on mineral imports produced in countries that do not adhere to equivalent US standards. This last policy would incentivize US space companies to source minerals domestically and from partner countries with high environmental and labor standards.

The Mineral-Intense Space Competition

Today, space is a competitive domain to a degree not seen since the space race between the United States and the Soviet Union in the 1950s.[2] In fact, the US military has officially declared space a warfighting domain.[3] In February 2024, Commander of US Space Command General Stephen N. Whiting warned that the space activities of China are augmenting its efforts to oust US military influence from the first island chain—roughly comprising Japan, Taiwan, part of the Philippines, and Indonesia—and the second island chain, which mainly includes Guam, the Northern Mariana Islands, and Palau.[4]

Indeed, an invasion of Taiwan by China—America's "pacing threat"—would likely feature space warfare and perhaps even the use of high-altitude electromagnetic pulse weapons to impair Taiwan's military defenses.[5] Possibly foreshadowing China's use of space warfare before an invasion of Taiwan, the Russian government hacked the US satellite company Viasat, which Ukraine's military relied on for communication, command, and control, on the eve of its 2022 invasion of Ukraine.[6]

If a Chinese invasion of Taiwan leads to a broader conflict with the United States, China would likely target US satellites as well. A recently revised People's Liberation Army doctrinal publication noted how the combat effectiveness of the US Air Force drops significantly without satellites.[7] Further, one 2022 analysis warns, "The People's Liberation Army has the incentives and capabilities to conduct preemptive attacks against US space

2. Charles Pope, "Raymond Praises Space Force Achievements and Purpose While Noting Ongoing Threats, Challenges," US Space Force, April 5, 2022, https://www.spaceforce.mil/.

3. Pope; Everett C. Dolman, "Space Is a Warfighting Domain," *Æther: A Journal of Strategy and Airpower* 1, no. 1 (Spring 2022), https://www.airuniversity.af.edu/; C. Todd Lopez, "Shanahan: Next Big War May Be Won or Lost in Space," US Department of Defense [DoD], April 9, 2019, https://www.defense.gov/; and Lloyd J. Austin III, "Senate Armed Services Committee Advance Policy Questions for Lloyd J. Austin, Nominee for Appointment To Be Secretary of Defense," US Senate Committee on Armed Services, January 19, 2021, 56, https://www.armed-services.senate.gov/.

4. Patrick Tucker, "Chinese Space, Nuclear Development Is 'Breathtakingly Fast,' DOD Officials Warn," Defense One, February 29, 2024, https://www.defenseone.com/; Yusuke Kawachi, "The Case of Japanese Land Power in the First Island Chain," *War on the Rocks*, February 13, 2023, https://warontherocks.com/; and Tom O'Connor and Naveed Jamali, "How US Plans for a Faraway Pacific War While China Plots to Disrupt It," *Newsweek*, April 20, 2023, https://www.newsweek.com/.

5. Gabriel Honrada, "Electric Shield: Taiwan Girding for a Chinese HEMP Attack," *Asia Times*, November 2, 2023, https://asiatimes.com/.

6. Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," *MIT Technology Review*, May 10, 2022, https://www.technologyreview.com/.

7. *In Their Own Words: Science of Military Strategy 2020* (Montgomery, AL: China Aerospace Studies Institute, January 2022), 379, https://www.airuniversity.af.edu/.

assets," including satellites.[8] As evidenced by its antisatellite test in 2007, China has also shown a willingness to use antisatellite weapons, regardless of the resulting space debris.[9] Thus, US-China space warfare could involve mineral-intensive space assets.

Mineral Compositions of Space Capabilities

The most common materials in US space assets—including satellites, direct-ascent antisatellite (DA-ASAT) weapons, and rocket bodies—are metallic materials, even more so than composite and ceramic materials.[10] Metallic materials with high strength-to-weight ratios, such as aluminum, titanium, and stainless steel, help reduce launch costs and increase payload capacity.[11] These minerals must also withstand extreme temperature fluctuations and are often alloyed together, providing additional performance benefits.[12]

Satellites

In a US-China conflict, satellites would function in an intelligence, surveillance, and reconnaissance role for both combatants, as well as an enabler of precision-guided missiles.[13] Possibly in anticipation of conflict with China in the space domain, the US military is creating satellite redundancy by launching large satellite constellations. The US Space Force's Space Development Agency aims for 1,000 satellites in orbit by 2026, and the US National Reconnaissance Office intends to "quadruple" its satellite fleet by 2033.[14]

Given the mineral intensity of satellites, these deployment targets have significant mineral demand implications. As one study notes, "The [satellite] structure mainly consists of [aluminum]-alloys, [titanium]-alloys, or stainless steel," adding that solar

8. Jiemin Hou, "Offensive Defense: People's Liberation Army Logic of Preemption in Space," *Æther: A Journal of Strategic Airpower & Spacepower* 1, no. 4 (Winter 2022): 12, 19, https://www.airuniversity.af.edu/.

9. Theresa Hitchens, "Debris from ASAT Tests Creating 'Bag Neighborhood' in Low Earth Orbit: Analyst," Breaking Defense, June 16, 2023, https://breakingdefense.com/.

10. Biliyar N. Bhat, "Aerospace Materials Characteristics," in *Aerospace Materials and Applications*, ed. Biliyar N. Bhat (Reston, VA: American Institute of Aeronautics and Astronautics, 2018), 1, https://ntrs.nasa.gov/.

11. Miria M. Finckenor, "Materials for Spacecraft," in *Aerospace Materials and Applications*, 8, https://ntrs.nasa.gov/.

12. Paul Gradl et al., "Advancement of Extreme Environment Additively Manufactured Alloys for Next Generation Space Propulsion Applications," *Acta Astronautica* 211 (2023): 483–85, https://doi.org/; and Finckenor, 9.

13. *2022 Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion* (Washington, DC: Defense Intelligence Agency, February 1, 2022), 9, https://www.dia.mil/.

14. Ramin Skibba, "The Space Force Is Launching Its Own Swarm of Tiny Satellites," *Wired*, August 14, 2023, https://www.wired.com/; and Theresa Hitchens, "NRO Plans 10-Fold Increase in Imagery, Signals Intel Output," Breaking Defense, October 10, 2023, https://breakingdefense.com/.

arrays contribute substantially to satellite mass. These arrays are predominantly composed of silicon, silver, aluminum, glass, germanium, and gallium (fig. 1).[15]

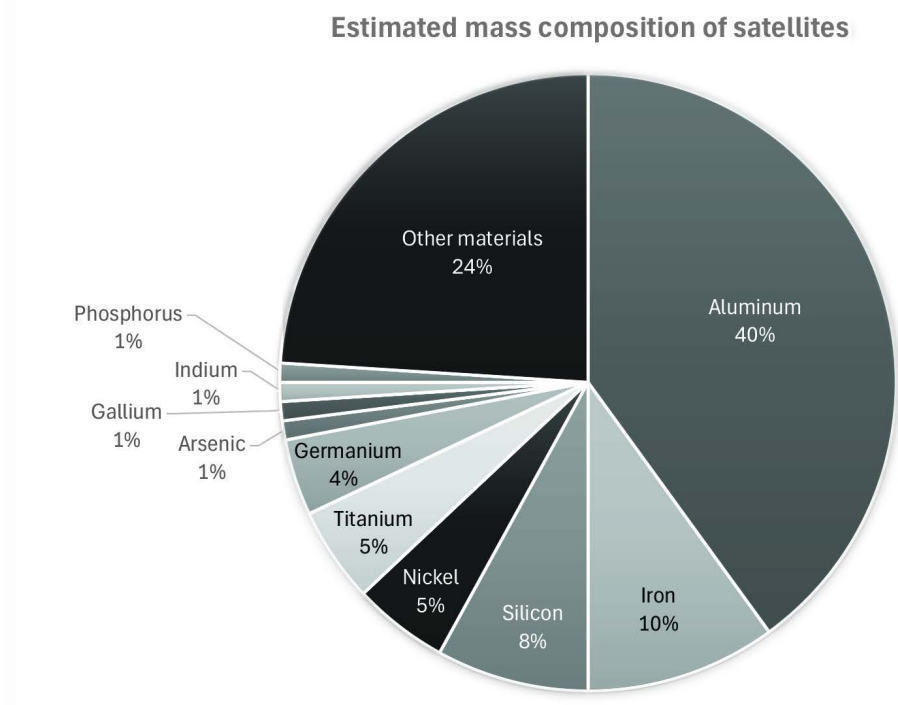

Figure 1. Estimated mass composition of satellites based on 2020 study[16]

Concerningly, the United States in 2023 had a high net import reliance, or the imports' share of domestic consumption, for many of these minerals: over 95 percent for titanium sponge metal, 57 percent for nickel, more than 50 percent for germanium—which the United States imports mainly from China—nearly 50 percent for silicon, and 44 percent for aluminum.[17] The United States also had a net import reliance of 100 percent for arsenic, 100 percent for gallium, 100 percent for indium, and 14 percent for phosphate rock.[18] Thus, it is highly dependent on imports of minerals necessary in satellites, exposing these mineral supply chains to disruption and cost risks.

15. Leonard Schulz and Karl-Heinz Glassmeier, "On the Anthropogenic and Natural Injection of Matter into Earth's Atmosphere," *Advances in Space Research* 67, no. 3 (2021), arXiv, August 29, 2020, 11, https://doi.org/.

16. Schulz and Glassmeier, 11.

17. Adam M. Merrill, "Aluminum," in *Mineral Commodities Summaries 2024* (Reston, VA: US Department of the Interior, US Geological Survey [USGS], January 2024), 32, https://doi.org/; Michele E. McRae, "Nickel," 124; Joseph Gambogi, "Titanium and Titanium Dioxide," 186; Emily K. Schnebele, "Silicon," 160; and Amy C. Tolcin, "Germanium," 80.

18. Micheal W. George, "Arsenic," in *Mineral Commodities Summaries,* 36; Brian W. Jaskula, "Gallium," 74; Andrew A. Stewart, "Indium," 90; and Stephen M. Jasinski, "Phosphate Rock," 134.

Direct-Ascent Antisatellite Weapons

Direct-ascent antisatellite weapons are an important counterspace capability. In a potential conflict, both China and the United States could target each other's satellites.[19] For example, the US military could use DA-ASAT weapons to target Chinese military satellites, hindering China's invasion effort and its possible long-range missile strikes on US forces in the Western Pacific.[20]

The US government currently has a self-imposed testing moratorium on destructive DA-ASAT weapons and reportedly prefers nonkinetic methods to disable adversarial satellites, but these weapons could prove highly effective among the available options in a US-China conflict.[21] While the US military does not have explicit DA-ASAT weapons, the Standard Missile-3 (SM-3) has demonstrated a DA-ASAT role as part of the Aegis Ballistic Missile Defense system. The Ground-based Midcourse Defense system and the Terminal High Altitude Area Defense system likely have similar DA-ASAT capabilities.[22]

The mineral-intensive SM-3 uses an aluminum guidance section, a stainless steel shell for third-stage components, and a graphite bismaleimide nose cone, which features an underlying thin molybdenum coating and a blunted titanium nose tip.[23] The SM-3 also uses rhenium for components exposed to high temperatures.[24]

For several of these minerals, the United States relies heavily on imports. For example, in 2023 it had an estimated net import reliance of 60 percent for rhenium and 100 percent for natural graphite, which it imports mainly from China.[25] Consequently, if the United States increases SM-3 production due to military expansion or

19. James A. Lewis, "Reconsidering Deterrence for Space and Cyberspace," in *Anti-satellite Weapons, Deterrence and Sino-American Space Relations*, ed. Michael Krepon and Julia Thompson (Washington, DC: Stimson Center, September 2013), 75, https://www.stimson.org/.

20. Mark A. Gubrud, "Chinese and US Kinetic Energy Space Weapons and Arms Control," *Asian Perspective* 35, no. 4 (2011): 625–26, http://www.jstor.org/.

21. Ching Wei Sooi, *Direct-Ascent Anti-Satellite Missile Tests: State Positions on the Moratorium, UNGA Resolution, and Lessons for the Future* (Broomfield, CO: Secure World Foundation and Swiss Existential Risk Initiative, October 2023), iii, https://swfound.org/; Laura Grego, "The Anti-Satellite Capability of the Phased Adaptive Approach Missile Defense System," *Federation of American Scientists* (Winter 2011): 4, https://pubs.fas.org/; and Gubrud.

22. Laura Grego, *A History of Anti-Satellite Programs* (Cambridge, MA: Union of Concerned Scientists, January 2012), 12, https://www.ucsusa.org/; and "Anti-Satellite Capability."

23. Gary A. Sullins, "Exo-atmospheric Intercepts: Bringing New Challenges to Standard Missile," *Johns Hopkins APL Technical Digest* 22, no. 3 (2001): 271, 273, https://secwww.jhuapl.edu/; and Scott D. Robinson, "Navy Theater-Wide Defense AEGIS LEAP Intercept (ALI)/STANDARD Missile 3 (SM-3) Flight Test Program Overview" (presentation, 6th Annual AIAA/BMDO Technology Readiness Conference, San Diego, CA, August 21, 1997), 6–7, https://apps.dtic.mil/.

24. National Center for Excellence in Metalworking Technology, *2003 Annual Report: Providing Metalworking Solutions to Enable Defense Transformation* (Mechanicsburg, PA: Concurrent Technologies Corporation, 2003), 9, https://apps.dtic.mil/.

25. Désirée E. Polyak, "Rhenium," in *Mineral Commodities Summaries*, 146; and Andrew A. Stewart, "Graphite (Natural)," 84.

munition attrition in a US-China conflict, these production lines could face disruption risks from Chinese mineral export controls or contested shipping routes.

Rocket Bodies

Rocket bodies are vital in enabling components in space and counterspace capabilities, powering satellites to their appropriate orbits and DA-ASAT weapons to their intended targets. A rocket body—which consists of a propulsion tank, engines, an internal and external structure, and a guidance and control system—must withstand extreme temperatures and pressure. Therefore, rocket bodies contain various alloys, including minerals such as aluminum, copper, hafnium, and lithium (fig. 2).[26]

Propulsion tanks are commonly made of AA2219 aluminum alloy; however, SpaceX's Super Heavy rocket booster consists of 300-series stainless steel.[27] For rocket engines, common alloys are nickel alloys such as Inconel 600 and Inconel 718, but SpaceX's Raptor rocket engines use a proprietary nickel alloy called SX500.[28] Wiring in rocket bodies is usually copper, while feedlines and other components are generally made of stainless steel, aluminum alloys, and titanium alloys.[29] Lastly, rocket nozzle extensions are often made of C-103 alloy, which consists of niobium, hafnium, and titanium.[30]

26. Daniel M. Murphy et al., "Metals from Spacecraft Reentry in Stratospheric Aerosol Particles," *Proceedings of the National Academy of Sciences of the United States of America* 120, no. 43 (2023): 2–3, https://doi.org/.

27. Rupendra Brahambhatt, "Why SpaceX's Starship Mega-Rocket Looks Unlike Anything the Company Has Ever Built Before," *Business Insider*, April 20, 2023, https://www.businessinsider.com/; and see Jim Rauf, "SpaceX 6: Starship and Super Heavy Booster" (lecture slides, University of Cincinnati, OH, 2023), 5, https://www.uc.edu/.

28. Schulz and Glassmeier, "Anthropogenic," 11; and Trevor Sesnic, "Raptor 1 vs Raptor 2: What Did SpaceX Change?," Everyday Astronaut, July 14, 2022, https://everydayastronaut.com/.

29. Daniel M. Murphy et al., "Metals from Spacecraft Reentry," 3; and Schulz and Glassmeier, 9.

30. Murphy et al., 3; and Omar R. Mireles et al., "Additive Manufacture of Refractory Alloy C103 for Propulsion Applications" (presentation, 2020 AIAA Propulsion and Energy Forum, August 24–26, 2020, virtual), 2, https://ntrs.nasa.gov/.

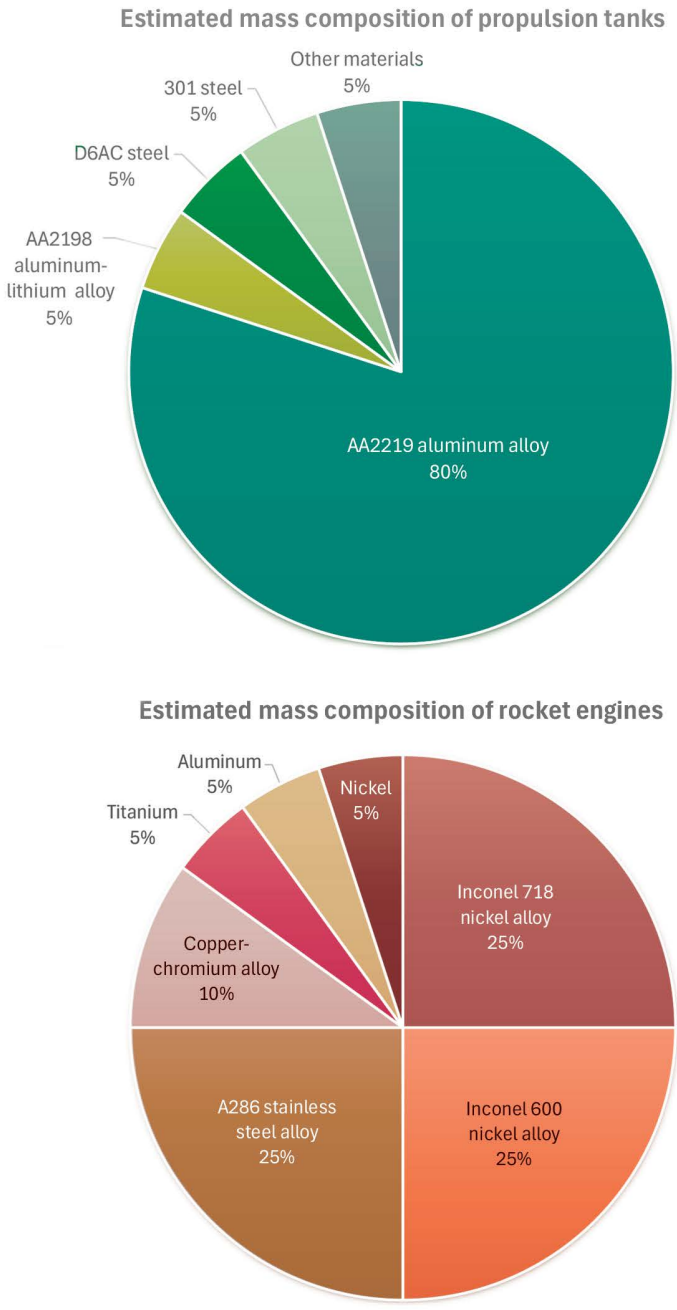

Figure 2. Estimated mass composition of propulsion tanks and rocket engines based on 2020 study[31]

31. Schulz and Glassmeier, "Anthropogenic," 9.

The United States relies on imports for these alloying elements as well, such as hafnium and niobium, subjecting them to the risks of supply chain disruption. Only two US companies produce hafnium metal; consequently, some hafnium comes from China and Russia.[32] With the limited supply of hafnium metal and its soaring demand in aerospace alloys, prices of this metal have increased dramatically, posing risks to the downstream production of space assets.[33]

Unlike with hafnium, the United States relies entirely on imports for its niobium consumption.[34] While America imports most of its niobium from Brazil, Chinese companies have ownership stakes in Brazilian production: a Chinese consortium has a 15 percent stake in Brazil's largest niobium producer, and a Chinese company—a subsidiary of CMOC—is the second largest niobium producer in Brazil.[35] As a result, the United States risks disruption of the mineral imports necessary to manufacture rocket bodies.

Mineral Supply Chain Risks

Russia and China, as major mineral producers, are linchpins in space asset supply chains. For example, Russia is a major global producer of titanium sponge, and the US government—while it has restricted imports of other Russia-produced minerals—has partly avoided restricting imports of Russian titanium given the aerospace industry's dependence on this supply.[36] During the Cold War, the Soviet Union was the world's largest titanium metal producer, and the US Central Intelligence Agency secretly procured Soviet titanium via third-party countries for Lockheed Martin when the company was building the SR-71 reconnaissance aircraft to spy on the Soviet Union.[37]

China has been recognized as a twenty-first century "mineral power" surpassing the United States, with its significant access to secure mineral supplies correlated with

32. Nedal T. Nassar, Elisa Alonso, and Jamie L. Brainard, *Investigation of US Foreign Reliance on Critical Minerals: US Geological Survey Technical Input Document in Response to Executive Order No. 13953 Signed September 30, 2020* (Reston, VA: USGS, December 7, 2020), 37, https://pubs.usgs.gov/; and Joseph Gambogi, "Zirconium and Hafnium," in *Mineral Commodities Summaries*, 204.

33. Gambogi, 205.

34. Chad A. Friedline, "Niobium (Columbium)," in *Mineral Commodities Summaries*, 126.

35. Abraham J. Padilla, "Niobium," in *2018 Minerals Yearbook* (Reston, VA: USGS, October 2021), 52.2, https://pubs.usgs.gov/; "Our History," CBMM [Companhia Brasileira de Metalurgia e Mineração], accessed April 16, 2024, https://cbmm.com/; and Jake Spring, "Hands Off Brazil's Niobium: Bolsonaro Sees China As Threat to Utopian Vision," Reuters, October 25, 2018, https://www.reuters.com/.

36. Adam Taylor, "Two Years after Start of Ukraine War, Russian Titanium Keeps Flowing to West," *Washington Post*, March 21, 2024, https://www.washingtonpost.com/; and Daniel Flatley and Jack Farchy, "Russian Metal Hit with Sanctions As US Blocks Deliveries to LME," Bloomberg, April 12, 2024, https://www.bloomberg.com/.

37. *The Soviet Titanium Industry and Its Role in the Military Buildup: A Research Paper* (Washington, DC: US Central Intelligence Agency, March 1985), iii, 1, https://www.cia.gov/; and Maya Carlin, "Titanium from Russia Was the Secret Ingredient in the SR-71 Blackbird," *National Interest*, December 3, 2023, https://nationalinterest.org/.

considerable military capabilities.[38] China is the world's dominant mineral producer and refiner and thus the key bottleneck in the mineral supply chain for space assets. To illustrate, China's Xinjiang Uyghur Autonomous Region produces about 45 percent of the world's polysilicon for crystalline silicon photovoltaic modules, whose space-grade versions power some space assets.[39] State support, especially financing, to Chinese mineral companies has helped China achieve this mineral dominance.

Importantly, the Chinese government financially supports not only domestic mineral projects but also overseas mineral projects.[40] For instance, Chinese state development banks (China Development Bank, Export-Import Bank of China) and Chinese state-owned commercial banks (Bank of China, Industrial and Commercial Bank of China) have financed coal-fired power plants at the Indonesia Morowali Industrial Park, which produces significant volumes of nickel-containing materials such as stainless steel.[41] Ultimately, China's influence over global production for many minerals gives it leverage over the supply chains of US space assets.

With its high mineral import dependence, the US space industry faces the associated risks of import disruptions such as export controls, which can restrict mineral availability and cause price volatility and which has stymied the production of US space assets. For example, China imposed export controls on gallium, germanium, and graphite in 2023, which significantly decreased these exports.[42] These minerals are used as inputs in space assets: gallium is used in semiconductors and aerospace applications; germanium is used in semiconductors as well as solar cells for satellites; and graphite is used in batteries, powdered metals, and refractory applications.[43]

US supply chains also face import disruption risks from other variables as well, including natural disasters, host government issues, and contested shipping routes. For instance, the attacks by Houthi rebels in Yemen on commercial ships transiting the Red Sea in late 2023 and early 2024 disrupted downstream supply chains such as automotive

38. Gregory Wischer and Morgan Bazilian, "The Rise of Great Mineral Powers," *Journal of Indo-Pacific Affairs* 7, no. 2 (March-April 2024), https://www.airuniversity.af.edu/.

39. Laura T. Murphy and Nyrola Elimä, *In Broad Daylight: Uyghur Forced Labour and Global Solar Supply Chains* (Sheffield, UK: Helena Kennedy Centre for International Justice, Sheffield Hallam University, 2021), 7, https://www.shu.ac.uk/; and Dave Doody, "Chapter 11: Onboard Systems," *Basics of Space Flight*, National Aeronautics and Space Administration, accessed April 16, 2024, https://science.nasa.gov/.

40. Debamanyu Das, "Role of the State in the Energy Transition: The Case of China and Lessons for the United States," SSRN, October 24, 2023, 21–22, 26–42, http://dx.doi.org/.

41. Pius Ginting and Ellen Moore, "Indonesia Morowali Industrial Park (IMIP)," People's Map of Global China, November 22, 2021, https://thepeoplesmap.net/.

42. "China Export Curbs Choke Off Shipments of Gallium, Germanium for Second Month," Reuters, October 19, 2023, https://www.reuters.com/; Siyi Liu and Dominique Patton, "China, World's Top Graphite Producer, Tightens Exports of Key Battery Material," Reuters, October 20, 2023, https://www.reuters.com/; and "Chinese Exports of Battery Material Graphite Plunge on Controls," Bloomberg, January 21, 2024, https://www.bloomberg.com/.

43. Brian W. Jaskula, "Gallium," in *Mineral Commodity Summaries 2024*, 74, https://pubs.usgs.gov/; Amy C. Tolcin, "Germanium," 80, https://pubs.usgs.gov/; and Andrew A. Stewart, "Graphite (Natural)," 84, https://pubs.usgs.gov/.

factories in Europe.[44] In the extreme case, a US-China conflict would severely disrupt mineral imports from Japan and South Korea, two refining powerhouses on which the United States heavily relies.[45] Hence, mineral import dependence creates supply chain risks to the production of US space assets, especially as the United States seeks to increase its space capabilities.[46]

Mineral import dependence also creates price risks to the US commercial space industry, which has become integral to US military space activities.[47] Import disruptions can restrict mineral availability in the United States, increasing mineral prices. Indeed, US space companies have noted the negative impact of high prices on their operations, such as when China restricted rare earth element exports in the early 2010s.[48]

A US Bureau of Industry and Security survey as early as 2014 found that the second leading issue for US operations related to titanium—a key mineral in space assets—was price volatility, with one titanium-related distributor saying costs can vary by 20 percent.[49] Further illustrating the importance of cost in manufacturing US space assets, SpaceX selected stainless steel instead of carbon fiber for the structural material in the Starship partly due to stainless steel's lower cost.[50]

---

44. Paul Wiseman and Mae Anderson, "Attacks on Ships in the Red Sea Are Disrupting Global Trade. Here's How It Could Affect What You Buy," AP, January 28, 2024, https://apnews.com/; and Matthew Beecham, "BriefCASE: Navigating the Red Sea Crisis, an Automotive Industry Perspective," S&P Global, February 15, 2024, https://www.spglobal.com/.

45. *Conflict over Taiwan: Assessing Exposure in Asia* (London: Economist Intelligence Unit, 2023), 1–3, 7, https://www.eiu.com/; Keita F. DeCarlo, "The Mineral Industry of Japan," in *2019 Minerals Yearbook: Japan* (Reston, VA: USGS, December 2023), 13.1, https://pubs.usgs.gov/; Jaewon Chung, "The Mineral Industry of the Republic of Korea," in *2019 Minerals Yearbook: Republic of Korea* (Reston, VA: USGS, June 2023), 15.1, https://pubs.usgs.gov/; and *Mineral Commodities Summaries*, 7.

46. Tucker, "Chinese Space."

47. Micah Maidenberg and Drew FitzGerald, "Musk's SpaceX Forges Tighter Links with US Spy and Military Agencies," *Wall Street Journal*, February 20, 2024, https://www.wsj.com/; Joey Roulette and Marisa Taylor, "Exclusive: Musk's SpaceX Is Building Spy Satellite Network for US Intelligence Agency, Sources Say," Reuters, March 16, 2024, https://www.reuters.com/; Audrey Decker, "Pentagon Eyes Starship, Designed for Mars, for Military Missions Somewhat Closer to Home," Defense One, March 15, 2024, https://www.defenseone.com/; Sandra Erwin, "SpaceX Launches US Missile-Defense Satellites," *SpaceNews*, February 14, 2024, https://spacenews.com/; and Jackie Wattles and Ashley Strickland, "SpaceX Falcon Heavy Launches X-37B Plane, One of the US Military's Most Fascinating Secrets," CNN, December 29, 2023, https://www.cnn.com/.

48. Bureau of Industry and Security (BIS), *US Space Industry 'Deep Dive': A Collaboration between the DOC and the USAF, NASA, and NRO, First Waypoint Preliminary Findings* (Washington, DC: US Department of Commerce, October 2012), 39, https://www.bis.doc.gov/.

49. BIS, *US Strategic Material Supply Chain Assessment: Titanium* (Washington, DC: Commerce Department, 2016), 70, 78, https://www.bis.doc.gov/.

50. Kenneth Chang, "What Is SpaceX's Starship? It's Really a Mars Ship," *New York Times*, March 14, 2024, https://www.nytimes.com/; Mike Wall, "Why Elon Musk Turned to Stainless Steel for SpaceX's Starship Mars Rocket," Space.com, January 13, 2019, https://www.space.com/; Brian Wang, "Estimate of the Cost Savings for SpaceX Stainless Steel Super Heavy Starship," *NextBigFuture.com*, January 28, 2019, https://www.nextbigfuture.com/; and Ryan D'Agostino, "Elon Musk: Why I'm Building the Starship Out of Stainless Steel," *Popular Mechanics*, January 22, 2019, https://www.popularmechanics.com/.

In addition, the lack of alternative mineral suppliers and mineral substitutes exacerbates supply risks for manufacturing US space assets. Military space applications require high-purity minerals from qualified suppliers, and transitioning to and certifying new suppliers can take up to 10 years, according to the Aerospace Industries Association.[51] Substituting limited availability minerals with readily available or cheaper minerals can compromise the effectiveness and safety of the space asset.[52] Given the highly demanding environment of space, such performance declines can render space assets inoperable.[53] In short, finding alternative mineral suppliers would likely cause manufacturing delays, and substituting different minerals would potentially cause performance declines in the space assets.

US Policy Options

To mitigate import disruption risks to the supply chains of US space assets, the US government should adopt the following policies: stockpile minerals vital to US space assets; provide concessional financing for US space companies to sign long-term, fixed-price mineral offtake agreements; and impose environmental and labor tariffs on mineral imports produced in countries that do not adhere to equivalent US E&L standards.

Mineral Stockpiling

First, the US government should stockpile minerals necessary in US space assets to mitigate mineral supply constraints and price volatility. In contrast with other industries like the automotive industry, the US space industry relies on smaller volumes of highly specialized materials.[54] Smaller demand enables easier stockpiling as smaller volumes would need to be acquired and stored. When limited mineral supplies or high mineral prices threaten to disrupt the production of US space assets, the government could sell stockpiled minerals to US space companies at fixed prices. China similarly sells stockpiled minerals to its strategic sectors, like the power sector, when high mineral prices threaten downstream production.[55]

The proposed stockpile would serve both strategic and economic purposes, similar to China's mineral stockpile.[56] While the US government currently employs the National

51. Aerospace Industries Association, *Securing the US Aerospace and Defense Critical Minerals Supply Chain*, white paper, June 14, 2023, 1–2, https://www.aia-aerospace.org/.

52. Karen L. Jones and Chloe I. Skorupa, *Mine Games: Securing America's Critical Mineral Supply* (El Segundo, CA: Center for Space Policy and Strategy, Aerospace Corporation, January 2024), 3, https://csps.aerospace.org/.

53. Jones and Skorupa, 1.

54. Aerospace Industries Association, "Securing the US Aerospace," 2.

55. Mai Nguyen and Min Zhang, "China to Release Copper, Aluminium and Zinc Reserves to Stabilise Prices," Reuters, June 16, 2021, https://www.reuters.com/; and Andy Home, "Learning to Live with (Talk of) Chinese State Metal Sales: Andy Home," Reuters, June 16, 2021, https://www.reuters.com/.

56. Gregory Wischer, "China Shows How Western Governments Should Stockpile Minerals," Strategist, March 6, 2024, https://www.aspistrategist.org.au/; and Wischer and Bazilian, "Great Mineral Powers."

Defense Stockpile, which contains many types of minerals, it is used for strategic—not economic—purposes, intended to reduce supply chain risks to the United States in the event of a national emergency, like a military conflict.[57] The National Defense Stockpile is prohibited from being used as an economic stockpile that sells minerals when prices are high and purchases minerals when prices are low.[58] Therefore, a new mineral stockpile specific to space assets and separate from that reserve should be created.

With the lack of US refining capacity for some minerals, the government would need to stockpile highly refined metal products that US space manufacturers could incorporate into their manufacturing lines without extensive processing. The relatively small mineral demand of individual space companies does allow some companies to undertake smaller batch refining operations. For example, SpaceX, which has its own metallurgy team and foundry, produces its proprietary SX500 alloy for the Raptor rocket engines.[59]

Nonetheless, most US space companies do not have the resources available to SpaceX; thus, the US government should stockpile highly refined metal products that could be integrated into manufacturing lines absent considerable processing. To mitigate the industry's limited access to refining capacity, the government should also consider how it can help companies procure the necessary processing equipment and technology to convert minerals into metals and chemicals for manufacturing space assets.

Concessional Financing

Second, the government should provide concessional financing for US space companies to sign long-term, fixed-price mineral offtake agreements.[60] This means that the mineral producer would agree to sell the space company a certain volume of the minerals at a set price over a specific time frame to attenuate mineral supply constraints and price volatility. US space companies sometimes face limited mineral availability and higher mineral prices due to other industries' larger demand and production cycles. For instance, the 2014 survey on titanium found that industry players expected the increased production of the Boeing 787 aircraft and Airbus A350 aircraft would increase titanium prices and lead times.[61]

---

57. Cameron M. Keys, *Emergency Access to Strategic and Critical Materials: The National Defense Stockpile*, R47833 (Washington, DC: Congressional Research Service, November 14, 2023) 43–44, https://crsreports.congress.gov/; BIS Request for Public Comments on the Potential Market Impact of the Proposed Fiscal Year 2025 Annual Materials Plan from the National Defense Stockpile Market Impact Committee, 88 Fed. Reg. 170, 60634 (Sept. 5, 2023), https://www.govinfo.gov/; *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017* (Washington, DC: White House, June 2021), 188, https://www.whitehouse.gov/; and Gregory Wischer and Jack Little, "The US Government Should Stockpile More Critical Minerals," *War on the Rocks,* September 27, 2023, https://warontherocks.com/.

58. Keys, 2; and BIS.

59. Brian Wang, "SpaceX Casting Raptor Engine Parts from Supersteel Alloys," *NextBigFuture*, February 18, 2019, https://www.nextbigfuture.com/.

60. See Wischer and Bazilian, "Great Mineral Powers."

61. BIS, *Titanium*, 85–86.

Likewise, a US space company in 2012 said it faced limited availability of carbon graphite due to competing demand from the production of the A350 and A380 aircraft.[62] In a competitive global market with high mineral demand, long-term offtake agreements at fixed prices could help secure minerals for the US space industry.

To further strengthen US mineral supply chains, government financing of offtake agreements should require borrowing space companies first to source domestically produced minerals if domestic supplies are available and then source foreign-produced minerals from geopolitically aligned countries. Critically, if the offtake agreements are signed with production facilities in East Asia, such as Japan and South Korea, these mineral supplies could be disrupted by US-China military tensions and a US-China conflict; therefore, the US government should condition the financing of offtake agreements with production facilities in East Asia on the desired materials not being produced in other partner countries such as Canada.

Lastly, mineral producers may prefer floating-price contracts over fixed-price contracts because they expect mineral prices to increase over the long term, but these producers also prefer long-term agreements due to guaranteed long-term revenue. Thus, mineral producers should be amenable to long-term, fixed-price mineral offtake agreements.

While the US government has not provided financing to companies to sign offtake agreements with mineral producers, the government has signed offtake agreements directly with mineral producers before. For example, in 1951, the US government contracted with the Calera Mining Company "for the purchase of 6.5 million pounds of cobalt-nickel alloy containing not less than 93 percent cobalt and not more than 7 percent nickel at a fixed premium price," from a mine in Lemhi County, Idaho.[63] Additionally, while uranium is not considered a critical mineral—which is defined as a nonfuel mineral—the US government has also directly procured domestic uranium ore.[64]

Regarding the structure of the proposed policy, one existing program that holds some similarities is financing from the US Export-Import Bank, which provides financing to foreign buyers of US goods. With the proposed policy, the US government would similarly provide financing to US space companies buying critical minerals.

Environmental and Labor Tariffs

Third, the US government should impose E&L tariffs on mineral imports produced in countries that do not adhere to equivalent US environmental and labor standards. Minerals produced in countries with lower standards have lower costs than minerals produced in the United States, which has strict regulations regarding waste management and carbon emissions. Such tariffs would offset this unfair cost advantage and

62. BIS, *Deep Dive*, 39.

63. Joseph H. Bilbrey Jr., *Colbalt: A Materials Survey*, Information Circular 8103 (Washington, DC: US Department of the Interior, Bureau of Mines, 1962), 21–22, https://dggs.alaska.gov/.

64. Michael Scott and Edward M. Heppenstall, "Atomic Energy – Uranium Procurement – Legal Aspects of the AEC Domestic Ore Purchase Program," *Michigan Law Review* 56, no. 5 (1958), https://repository.law.umich.edu/.

incentivize US space companies to source minerals primarily from the United States and secondarily from partner countries, such as Australia.

The government should also ban mineral imports produced in a manner suspected of violating environmental protections and labor rights. For example, the Uyghur Forced Labor Prevention Act already in place seeks to prevent goods made with forced labor in China's Xinjiang region from entering the United States.[65] The US government should seek to do the same for minerals regarding environmental and labor practices in other regions. For instance, it should aim to prevent nickel and cobalt produced in Indonesia's Sulawesi Island and North Maluku from entering the United States due to environmental abuses.[66] Imposing tariffs for environmental and labor reasons has better chances of garnering bipartisan political support. Ultimately, E&L tariffs and import bans should incentivize US space companies to source minerals domestically and from partner countries with high environmental and labor standards.

Conclusion

US space assets are mineral-intensive. Satellites, DA-ASAT weapons, rocket bodies, and other assets all require substantial volumes and various types of minerals. But the supply chains for minerals vital in US space assets face risks of mineral import disruptions such as export controls and interrupted shipping lanes. Such import disruptions can restrict mineral availability and cause price volatility, negatively impacting the production of US space assets. These conditions could prove particularly detrimental to the US military in a conflict with China, which itself is a major supplier of minerals to the United States.

To help mitigate risks to these vital mineral supply chains, the US government with the US Space Force as the primary coordinator should stockpile minerals critical to US space assets; provide concessional financing for US space companies to sign long-term, fixed-price mineral offtake agreements; and impose E&L tariffs on mineral imports produced in countries that do not adhere to equivalent US E&L standards. Such secure access to sufficient mineral volumes is critical for accelerated and uninterrupted production of US space assets and the preservation of US space leadership. Æ

---

65. An Act to Ensure That Goods Made with Forced Labor in the Xinjiang Uyghur Autonomous Region of the People's Republic of China Do Not Enter the United States Market, and for Other Purposes, Pub. L. No. 117-78, 135 Stat. 1525 (2021), https://www.govinfo.gov/.

66. Endang Naryono, "Nickel Mine Exploitation in Indonesia, between a Blessing and a Disaster of Environmental Damage," preprint, OSF Preprints, September 19, 2019, https://doi.org/; and *Nickel Unearthed: The Human and Climate Costs of Indonesia's Nickel Industry* (Berkeley, CA: Climate Rights International, January 2024), https://cri.org/.

EMERGING LAWS AND NORMS FOR AI FACIAL RECOGNITION TECHNOLOGY

ALISON LAWLOR RUSSELL

The explosive growth of facial recognition technology has exceeded the ability of existing legal frameworks related to privacy around the world to adequately safeguard individuals and human rights. Laws governing the use of this technology and collection of biometric information range from nonexistent in some countries to robust in others, and in some cases, these laws favor nondemocratic regimes and threaten individuals' privacy. At this critical juncture, the United States should work with its Allies and partners to establish and promote norms protecting human rights as governments and the private sector take advantage of this increasingly robust technology.

Innovation and technological development proceed much faster than policy or norm development, and it can be a challenge for decisionmakers to modernize legislation to keep pace with social and technological changes. The adoption of a new technology, in the field of biometrics for example, leads to new practices. New laws may be implemented alongside new technologies, which in turn may affect norms and expectations of surveillance and privacy. With the rise of artificial intelligence (AI) and surveillance technologies, many governments have invested in and implemented facial recognition surveillance technology for a variety of reasons, such as public safety, pandemic-related policies, counterterrorism efforts, and domestic control.

Since 2016, there has been a dramatic increase in the use of such surveillance technologies, and it is unclear what laws and policies are being created to govern their use and the use of other biometric data, particularly in regard to privacy and human rights. In recognition of this, the UN High Commissioner for Human Rights called for a moratorium in 2021 on the use of artificial intelligence and facial recognition in public spaces until safeguards for rights are established.[1]

Dr. Alison Russell is the chair and associate professor of the Political Science & Public Policy Department and the director of the international studies program at Merrimack University, Massachusetts. She is the author most recently of Strategic A2/AD in Cyberspace *(Cambridge University Press, 2017).*

1. Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/48/31, United Nations (website), September 13, 2021, https://www.ohchr.org/.

Facial recognition technology impedes on individual privacy, which is a human right that includes privacy of one's information and from observation, the moral values of autonomy—where an individual can make choices consistent with their sense of self, not because they are being monitored and perhaps threatened with punishment—and privacy for personal projects and plans. Collective privacy maintains a power balance between the state and society, particularly in liberal democratic regimes.

The impact of surveillance technology's global proliferation on laws and norms concerning privacy and human rights presents a new dimension for how technology adoption and risk are considered. As new laws are constructed, new norms will also emerge in international law applicable to cyberspace and technology.

By examining the use of AI facial recognition technology (FRT) by individual countries, this article observes how different states approach their obligations regarding privacy and human rights and looks for patterns or trends that may impact global norm development for this technology. An analysis of emerging FRT laws and policies in various countries finds both democratic and nondemocratic nations are approaching the technology in a number of different ways, with some adopting laws to govern the use of this technology.

At the same time, many countries, regardless of government type, have yet to adopt such laws, and it is unclear if and when they will. Current laws that protect human rights and privacy are thus insufficient to address critical aspects of this technology. Further, and critically, democracies that have failed to create laws and policies protecting citizens from FRT have promulgated legal voids in a similar manner as nondemocratic regimes that seek to protect those in power.

Methodology

This article employs a comparative approach to answering the main questions and investigating the conditions that may contribute to countries adopting laws that restrict privacy and expanding the use of facial recognition technology. Nineteen countries plus the European Union (EU) were selected to represent diversity in regime type (democracies and nondemocracies), geographic location, and population size.

This research is primarily focused on national laws that govern the state's use of FRT, but where possible, it also collects data on how this technology is being used within the countries and any restrictions of private-sector use of the technology. In addition, it is noted when countries regulate 1:1 and 1:N FRT differently. With 1:1 FRT, a subject's photo is matched to a specific image in a database to determine if the images are of the same person and is frequently used by applications for authentication or verification during a login process. In contrast, 1:N FRT is used to compare the subject's photo to multiple images in a database to see if any of them are a match.[2]

This research is concerned with AI facial recognition technology legislation since 2016. That year is not a decisive turning point, but rather an approximate midway

2. "Accurate 1:1 Face Matching," FACIA (website), accessed April 24, 2024, https://facia.ai/.

point in the recent global development and proliferation of FRT. Facial recognition technology using AI in social media began in 2010 with Facebook allowing users to tag and identify people in photos, and use of the technology accelerated from there. The iPhone X, released in 2017, used FRT to unlock the phone, thereby bringing this technology into the daily lives of people.[3]

The year 2016 was selected as a reference point because while AI FRT was still relatively new at that time, it had been in existence long enough for governments to experiment integrating it with existing practices as well as to begin considering the legal implications of it. For example, in 2011 the Federal Bureau of Investigation launched the FRT component of its Next Generation Identification Interstate Photo System (NGI-IPS) with a database of over 10 million images. In 2016, the Government Accountability Office revealed that the NGI-IPS also gained access to and included over 400 million noncriminal civilian images in its database. By 2019, the database had over 640 million images.[4]

Many countries have data protection laws that were passed in the late 1990s and early 2000s. Yet laws created in that time period are less likely to address concerns that are relevant for the way FRT is deployed in the public and private sector today. Specifically, most do not address the wide-scale use of biometric data collection and AI, the need for oversight, or the requirements for storage and protection of sensitive biometric data, such as fingerprints, iris scans, and facial images.

As the technology evolved into the 2010s and beyond, there was a growing recognition of the capabilities of AI-enabled FRT and the legislative measures that might be needed to regulate its use. The COVID-19 pandemic and the use of this technology to enforce lockdown measures in many countries accelerated the use of AI-enabled FRT and the public's awareness of it.

Additionally, the technology has also evolved, further surpassing previous limitations of machine-learning models, which struggled with effectiveness when using large databases. These limitations have been overcome by FRT models that harness deep learning and make them more effective with larger databases, including models that scrape vast numbers of images from social media and the internet as a whole.[5] As this technology has advanced, so too have the efforts of activists and lawyers who are concerned with its impacts on privacy, democracy, and human rights.

3. "A Brief History of Facial Recognition," NEC (website), May 12, 2022, https://www.nec.co.nz/.

4. Samuel Brice, "A Short History of Facial Recognition," Medium, November 7, 2020, https://samdbrice.medium.com/.

5. FACIA, "Face Matching."

Country Studies

Argentina

In Argentina, city, state, and federal legislatures coexist and sometimes contradict each other. Argentina's federal law on data protection, enacted in 2000, fails to consider AI FRT, other biometric data, or the collection of other sensitive personal data.[6] In 2019, Buenos Aires implemented the Fugitive Facial Recognition System, but it was suspended in 2020 during the COVID-19 pandemic due to reduced effectiveness with masked faces.[7]

In September 2022, a trial judge declared this system unconstitutional because of the privacy risks it posed. Specifically, the judge found that the rights to privacy, intimacy, and data collection have collective relevance in the context of public surveillance and law enforcement. The court prohibited the operation of the Fugitive Facial Recognition System until the control and oversight mechanisms required by law are put in place.[8] Other cities currently have plans to move ahead with different facial recognition systems.[9]

Australia

In Australia, the government and civil society use facial recognition technology widely. There are limited restrictions on it and no AI-specific legislation. The proposed Identity Verification Services legislation calls for the curtailing of 1:1 FRT, such as those employed by apps for authentication during the login process. It does not regulate the use of biometric information and identity matching that falls outside of the scope of the legislation, such as 1:N FRT that is already in widespread use.[10] New legislation to regulate the "high-risk" usage of AI, such as in law enforcement or hiring practices, while minimizing restrictions on "low risk" usage, such as with chatbots, is under consideration.[11]

---

6. Carolina Caeiro, *Regulating Facial Recognition in Latin America* (London: Chatham House, November 11, 2022), https://www.chathamhouse.org/.

7. Maria Badillo, "Judge Declares Buenos Aires Fugitive Facial Recognition System Unconstitutional," *Future of Privacy Forum* [blog], September 30, 2022, https://fpf.org/.

8. Badillo; and *Juzgado de 1ra Instancia en lo Contencioso Administrativo y Tributario No 4 Secretaría* N°7 *Observatorio de Derecho Informatico Argentino O.D.I.A. y Otros contra GCBA sobre Amparo – Otros* (Buenos Aires, Argentina: Poder Judicial Ciudad de la Buenos Aires, September 2022), https://www.cels.org.ar/.

9. Karen Naundorf, "The Twisted Eye in the Sky over Buenos Aires," *Wired*, September 13, 2022, https://www.wired.com/.

10. Shivaune Field, "Facial Recognition Is Everywhere – But Australia's Privacy Laws Are 'Falling Way Behind,' " *Forbes*, September 28, 2023, https://www.forbes.com.au/.

11. Phil Mercer, "Australia Outlines Plan to Manage the Rise of Artificial Intelligence," VOA [Voice of America], January 17, 2024, https://www.voanews.com/; and *Government Response to the Privacy Act Review Report* (Barton, Australia: Australian Government, Attorney General's Department, September 28, 2023), last updated February 16, 2024, https://www.ag.gov.au/.

Belgium

Belgium banned the use of facial recognition and other biometrics-based video surveillance technology by the private sector for nonpolice use in 2018.[12] Yet there are no laws that govern the use of FRT by the government. There has been public debate and demands by human rights groups to regulate the government's use of facial recognition technology, but legislation has not been passed yet.[13]

Brazil

Brazil's General Data Protection Law makes data protection a fundamental right in Brazil, but it does not apply to data collection carried out for the purposes of public safety, national security, and defense or for investigation or prosecution of criminal offenses.[14] There have been several federal commissions formed to advise on the drafting of a bill to regulate AI as well as civil-society led demonstrations against the use of FRT in public spaces. The existing national legislation enshrines the right to privacy, so any future discussions and legislation on FRT will be grounded in the General Data Protection Law and protection of constitutional rights.[15]

Canada

Canadian law requires express opt-in consent for the use of FRT by private companies. Privacy regulators have called for more national legislation to regulate the use of this technology in Canada, as some laws are local or provincial. New legislation that addresses the shortcomings of Bill C-27, which includes the Consumer Privacy Protection Act and the Artificial Intelligence and Data Act, is before the Canadian parliament for consideration in 2024. Yet privacy experts charge that the proposed amendments to the existing legislation are inadequate because they not only fail to provide special protections for biometric information, but they also do not flag biometric data as "sensitive information" or define sensitive information at all.[16]

12. Charles Rollet, "Belgium Bans Private Facial Surveillance," IPVM, July 6, 2018, https://ipvm.com/.

13. Act on the Protection of Natural Persons with Regard to the Processing of Personal Data [unofficial translation], Data Protection Authority, Government of Belgium, July 30, 2018, https://www.dataprotectionauthority.be/; and Maïthé Chini, " 'Protect My Face': Facial Recognition Petition Demands Ban in Brussels Public Spaces," *Brussels Times*, March 15, 2023, https://www.brusselstimes.com/.

14. "Data Protection Laws of the World: Brazil," DLA Piper, last modified January 28, 2023, https://www.dlapiperdataprotection.com/; and Rennó Penteado Sampaio Advogados, trans., "Brazilian General Data Protection Law (LGPD, English translation)," IAPP [International Association of Privacy Professionals], October 2020, https://iapp.org/.

15. Caeiro, *Regulating Facial Recognition*.

16. Howard Solomon, "Proposed Privacy, AI Legislation Doesn't Limit Business Use of Facial Recognition, Complain Rights Groups," IT World Canada, November 1, 2023, https://www.itworldcanada.com/.

China

China is the most surveilled country in the world and helped to fuel the explosion of facial recognition technology globally. In August 2023, the Chinese government issued rules to oversee the management of FRT. The Cyberspace Administration of China stated that FRT can only be used when there is a specific purpose and necessity and must be accompanied by strict protective measures. The Cyberspace Administration states biometric data should only be used with the individual's consent and other nonbiometric means of identification should be used when they are equally effective.[17] FRT should be reserved for the purpose of maintaining public safety, although there are circumstances in which administrative use of this technology does not require individual consent.[18]

This law attempts to protect citizens from capitalist surveillance but does not restrict the use of government surveillance or use of FRT on the general population. It also encompasses broad exceptions for national security and public safety. Overall, it enables a continued state of surveillance and overt government exceptionalism to restrictions on individuals' privacy, but it also grants individuals new rights to protect their privacy and personal data from businesses that stand to profit from them.[19]

European Union

In December 2023, the EU agreed to new rules to regulate the use of AI and biometric surveillance. The regulations are being hailed as a regulatory breakthrough and a global standard.[20] According to the new agreement, governments can only use real-time biometric surveillance in public spaces in certain circumstances, such as "the prevention of genuine, present, and foreseeable threats . . . and searches for people suspected of the most serious crimes." The indiscriminate scraping of facial images from the internet or closed-circuit television (CCTV) is prohibited, and consumers "would have the right to launch complaints and receive meaningful explanations."[21]

---

17. "Provisions on Security Management in the Application of Facial Recognition Technology (Trial) (Draft for Comment)," China Law Translate, August 2023, https://www.chinalawtranslate.com/; and Josh Ye, "China Drafts Rules for Using Facial Recognition Technology," Reuters, August 7, 2023, https://www.reuters.com/.

18. Evelyn Cheng, "China Releases Plans to Restrict Facial Recognition Technology," CNBC, August 8, 2023, https://www.cnbc.com/.

19. Johanna Costigan, "New Chinese Facial Recognition Regulations Could Shield Citizens from Surveillance Capitalism," *Forbes*, August 9, 2023, https://www.forbes.com/.

20. Adam Satariano, "E.U. Agrees on Landmark Artificial Intelligence Rules," *New York Times*, December 8, 2023, https://www.nytimes.com/.

21. European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, February 2, 2024, EU Artificial Intelligence Act (website), https://artificialintelligenceact.eu/; and Foo Yun Chee, Martin Coulter, and Supantha Mukherjee, "Europe Agrees Landmark AI Regulation Deal [*sic*]," Reuters, December 11, 2023, https://www.reuters.com/.

The European Parliament voted on the final legislation in March 2024, which will enter into force in summer 2024.[22]

France

In March 2023, France passed a controversial law to allow police to use surveillance cameras and AI for public safety ahead of the 2024 Olympics. The law allows law enforcement to identify threats "such as dangerous crowd movements and unattended bags," but facial recognition technology is not permitted.[23] France's new law varies in certain ways from the EU's new AI Act, so there may be a potential clash between EU and French laws.[24]

India

India does not have laws that directly govern the use of facial recognition technology, as the Personal Data Protection Bill of 2019 and Information Technology Act of 2000 do not address it.[25] AI FRT is used in many parts of the country to solve crimes. The government is promoting a "smart cities" approach through the use of drones, AI-enabled CCTV, and FRT that appears to enjoy support across the political spectrum.[26]

In 2022, the Criminal Procedure (Identification) Act took effect, expanding the government's authority to collect biometric and behavioral data for people who are arrested, have court dates, or are convicted criminals. India's National Crime Records Bureau is looking to build one of the largest facial recognition systems in the world. It seeks to create a database of "mugshots of criminals, passport photos, and images collected by agencies such as the Ministry of Women and Child Development," that could be matched to images from CCTV cameras across the country.[27]

---

22. Caitlin Andrews, "European Parliament Approves Landmark AI Act, Looks Ahead to Implementation," IAPP, March 13, 2024, https://iapp.org/; Joe Jones, "EU AI Act: Next Steps for Implementation," IAPP, last updated January 2024, https://iapp.org/; and Lisa Peets, Marianna Drake, and Marty Hansen, "EU AI Act: Key Takeaways from the Compromise Text," Covington, *Inside Privacy* [blog], February 28, 2024, https://www.insideprivacy.com/.

23. Relatif aux Jeux Olympiques et Paralympiques De 2024 - (N° 809) [Relating to the 2024 Olympic and Paralympic Games - (No. 809)], Amendment No. CL400, National Assembly of the Republic of France, March 4, 2023, https://www.assemblee-nationale.fr/; and Peter O'Brien, "France Passes Controversial AI Surveillance Bill Ahead of 2024 Olympics," France 24, March 24, 2023, https://www.france24.com/.

24. Masha Borak, "French Senate Votes in Favor of Public Facial Recognition Pilot," BiometricUpdate.com, June 14, 2023, https://www.biometricupdate.com/.

25. Pavan Duggal, "Facial Recognition in India – Some Legal Challenges," CyberLaws.net, accessed April 24, 2024, https://cyberlaws.net/; and Rishabh R. Jain, "Facial Recognition Wielded in India to Enforce COVID Policy," AP, December 20, 2022, https://apnews.com/.

26. Jain.

27. Julie Zaugg, "India Is Trying to Build the World's Biggest Facial Recognition System," CNN, October 18, 2019, https://www.cnn.com/.

Israel

In September 2023, the Israeli government received cabinet approval for its bill to place FRT cameras in public places during events, such as protests, as long as a police officer is convinced it does not amount to the "undue invasion" of any individual's privacy.[28] The legislation allows for the use of facial recognition cameras and their data "to prevent, thwart, or uncover serious crime" and the individuals involved.[29]

Human rights organizations, such as Amnesty International, have alleged that Israel is increasingly using FRT to surveil and track movements of Palestinians in the West Bank and East Jerusalem.

Since the attacks on October 7, 2023, the Israeli military has used an expansive facial recognition program to search for hostages taken by Hamas, track Palestinians in Gaza, and identify anyone with ties to Hamas or other militant groups. Yet the program has, at times, wrongly identified civilians as militants. The Israeli Defence Forces does not dispute the use of the mass surveillance program but states it is carrying out "necessary security and intelligence operations."[30]

Japan

Japanese technology is often at the forefront of innovation, and FRT is widespread in Japan. With the addition of its new extension, Osaka Station has been billed as the most high-tech train station in the world, with a trial for facial recognition scans for passenger entry underway. In other parts of Japan, drone delivery of medicines is being tested with FRT embedded to verify that an authorized person receives the delivery.[31]

Japan recognizes facial features as biometric data that are protected by the Personal Information Protection Code, which requires consent of the individual. But in practice, the private sector uses facial recognition cameras in large areas where consent of every individual is not possible and police have access to the data.[32] It appears Japan does not have any legal requirements concerning the handling of facial recognition data, except that FRT must be accompanied by a public notice of the purpose of the data, or notification of the subject whose information is being collected.[33]

---

28. Josh Breiner, "Israeli Gov't Pushes Bill for Facial Recognition Surveillance Cameras in Public Spaces," Haaretz, September 18, 2023, https://www.haaretz.com/.

29. Carrie Keller-Lynn, "Ministers Back Bill to Legalize Widespread Police Use of Facial Recognition Tech," *Times of Israel*, September 18, 2023, https://www.timesofisrael.com/.

30. Sheera Frenkel, "Israel Deploys Expansive Facial Recognition Program in Gaza," *New York Times*, March 27, 2024, https://www.nytimes.com/.

31. Joel R. McConvey, "Trains, Drones and Robotic Feels: Japan Deploys Facial Recognition across Sectors," BiometricUpdate.com, April 14, 2023, https://www.biometricupdate.com/.

32. Act on the Protection of Personal Information (Act No. 57 of 2003) [unofficial translation], Cabinet Secretariat [of Japan], 2003, https://www.cas.go.jp/.

33. Yazukazu Akada, "Review Launched into Rules Governing Facial Recognition Data," *Asahi Shimbun*, December 22, 2021, https://www.asahi.com/; and Sameshima Shigeru, "Privacy Measures of Biometrics Businesses," *NEC Technical Journal* 13, no. 2 (2018), https://www.nec.com/.

Myanmar

In Myanmar, surveillance technology was adopted without public consultation and is used to identify people and license plates. There are over 300 AI-equipped surveillance cameras that are capable of facial recognition across the capital city as part of the Safe City Initiative. National law requires the collection of biometric data when purchasing a smartphone, leading to the creation of a national database on biometric data.[34]

Russia

Russia's Law on Personal Data protects information related to an identifiable person and requires consent of the individual for the collection of biometric data through facial recognition technology. Yet laws on public security and crime prevention, such as the Law on Experimenting with Artificial Intelligence, provide exceptions to this requirement for consent, rendering it ineffective. According to human rights activists, the law does not provide any mechanisms for judicial or public oversight for surveillance collection and technologies and therefore lacks appropriate or sufficient guardrails to prevent the misuse of the technology and data.[35]

Human rights organizations assert that facial recognition technology is widely used throughout Russia with no regulation, oversight, or data protection. Furthermore, Russian authorities have begun to implement silhouette recognition technology in instances when the face is not visible. The lower house of the Duma passed legislation in December 2022 that set up a legal framework for collection, storage, and management of biometric data and outlawed the forceful collection of biometric data—face and voice—from any individual.[36]

South Africa

Facial recognition technology is legal, widespread, and largely unregulated in South Africa. In February 2021, the constitutional court of South Africa found the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 to be unconstitutional because it failed to provide adequate safeguards to protect the right to privacy.[37]

---

34. Katya Pivcevic, "Police Facial Recognition Use in Belarus, Greece, Myanmar Raises Rights, Data Privacy Concerns," BiometricUpdate.com, March 15, 2021, https://www.biometricupdate.com/; and Luana Pascu, "Myanmar to Introduce Mandatory Biometric Data Collection for Massive National Database," BiometricUpdate.com, December 6, 2019, https://www.biometricupdate.com/.

35. *2022 Country Reports on Human Rights Practices: Russia* (Washington, DC: US Department of State, Bureau of Democracy, Human Rights, and Labor, 2023), https://www.state.gov/.

36. Ayang Macdonald, "Russian Lawmakers Okay Legal Framework for Biometric Data Collection and Processing," BiometricUpdate.com, December 23, 2022, https://www.biometricupdate.com/.

37. Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others CCT278/19 & CCT279/19, Constitutional Court of South Africa, February 4, 2021, https://www.saflii.org/.

In May 2021, South Africa's Department of Home Affairs drafted an identity management policy to grant police "unfettered access" to citizens' biometric data without a court order. The policy proposed that all biometric data of all citizens should be centralized in a database and that an automated biometric identification system be created, but South Africa does not have any laws regulating police use of facial recognition software or related surveillance technology.[38]

South Korea

South Korea has promoted facial recognition technology through its ministries and local governments in recent years but does not appear to have laws or policy providing its oversight or regulation. In January 2023, the National Human Rights Commission of Korea warned against the dangers of implementing FRT without legislative regulations in place and asked the speaker of the National Assembly to delay the implementation of this technology in public institutions until a law is created.[39]

The commission recommended to the prime minister that all real-time FRT in public spaces be suspended until relevant laws are created to protect privacy and human rights. Additionally, the commission recommended that real-time facial recognition should be generally prohibited, except in extraordinary circumstances "based on clear and imminent public interest . . . such as searching for missing children."[40]

United Arab Emirates

The United Arab Emirates (UAE) passed a law in February 2021 allowing the use of facial recognition technology in certain private and government sectors to verify the identity of individuals and reduce paperwork.[41] This legislation came after several emirates implemented policies using FRT. In 2021 the UAE implemented a national digital identity and solutions system for citizens and residents, called the "UAE Pass," that uses facial recognition and smartphones to provide government services.[42]

---

38. Ayang Macdonald, "South Africa's Proposed New Biometrics Policy Meets Sharp Criticism," BiometricUpdate.com, May 17, 2021, https://www.biometricupdate.com/.

39. Alessandro Mascellino, "South Korea Privacy Watchdog Warns against Public Facial Recognition Deployments," BiometricUpdate.com, January 25, 2023, https://www.biometricupdate.com/; and Chai Yoon-tae, "Korean Rights Watchdog Advocates Curbs on Government's Use of Facial Recognition Data," *Hankyoreh*, January 26, 2023, https://english.hani.co.kr/.

40. Chai.

41. Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data ('the Law') [United Arab Emirates], September 20, 2021, https://www.dataguidance.com/; Ayang Macdonald, "UAE Cabinet Approves Trial of Facial Recognition for Private Sector Services," BiometricUpdate.com, February 17, 2021, https://biometricupdate.com/; and Jay Hilotin and Vijith Pulikkal, "UAE Approves Facial Recognition in Some Key Sectors: How the Technology Is Changing Our World," *Gulf News*, March 13, 2021, https://gulfnews.com/.

42. "UAE Government to Employ Biometric Face Recognition to Register Customers under 'UAE Pass' App," Emirates News Agency, April 4, 2021, https://wam.ae/.

United Kingdom

Facial recognition has been controversial in the United Kingdom for years. There is no specific facial recognition law in the UK, but the Data Protection Act of 2018 establishes some responsibilities surrounding its use.[43] In 2020, a British court ruled that the use of FRT to create a watchlist for the South Wales police force was unlawful and violated the human rights of the people whose data was collected and outlined issues that would need to be addressed for it to be lawful.[44] Privacy and civil liberty groups, experts, and lawmakers have called for a ban on live or real-time FRT in the UK, particularly in public places, because they claim it infringes on human rights and privacy.[45]

United States

The United States does not have federal laws governing the use of FRT, so some states, cities, and counties have developed their own, creating a patchwork of laws throughout the country. Twenty of the 42 federal law enforcement agencies use FRT. The majority of US states do not have restrictions on its use, but thirteen states do—Washington, Vermont, Maine, Virginia, New York, California, New Hampshire, Oregon, Utah, Massachusetts, Illinois, Texas, and Colorado—although these laws vary on whether they prohibit or regulate government or private sector use of FRT.

Cities such as Portland, Oregon and Baltimore have banned commercial use of this technology, while Portland and other cities, including Boston, San Francisco, and New Orleans, have enacted full bans on governmental use of FRT.[46] There have been several proposals in the US Congress to regulate the use of FRT, but none have gained enough support to move forward.[47]

Venezuela

Venezuela does not appear to have any laws or regulations pertaining to facial recognition technology or data protection. The Venezuelan government engages in robust surveillance activities and lacks independent oversight of the state's surveillance of citizens. The Maduro regime requires participation in government surveillance and data

43. Data Protection Act 2018 [United Kingdom], 2018 c.12, https://www.legislation.gov.uk/.

44. R v Chief Constable of South Wales Police, (2020) EWCA Civ 1058, https://www.judiciary.uk/; and "Facial Recognition Cameras - What Your Rights Are," *DAS Law* [blog], May 3, 2023, https://www.daslaw.co.uk/.

45. Matt Burgess, "Police Use of Face Recognition Is Sweeping the UK," *Wired*, November 9, 2023, https://www.wired.com/; and Vikran Dodd, "UK Police Use of Live Facial Recognition Unlawful and Unethical, Report Finds," *Guardian*, October 27, 2022, https://www.theguardian.com/.

46. Palash Basu and Jenny Holmes, "Facial Recognition Systems Regulation: Outlook for 2022," Bloomberg Law, December 23, 2021, https://news.bloomberglaw.com/.

47. Tate Ryan-Mosley, "The Movement to Limit Face Recognition Tech Might Finally Get a Win," *MIT Technology Review*, July 20, 2023, https://www.technologyreview.com/.

collection programs to access government services and subsidies, including a virtual wallet to receive pension payments that is integrated with a biometric payment system operated by Banco de Venezuela.[48] Facial recognition technology is used by the government, police, banking, and in transportation, such as at airports and on trains.[49]

Zimbabwe

Zimbabwe also engages in robust surveillance activities yet does not have laws to specifically regulate or limit the use of FRT. Facial recognition technology is being used by government, police, banking, and transportation sectors, such as for buses, trains, and airports.[50] There are no laws that limit or restrict surveillance activities, and FRT is not covered under the Interception of Communications Act (2007), the legislation that legitimized surveillance in Zimbabwe.[51] A data protection law passed in 2021 has been criticized for having multiple shortcomings, while the government maintains that the purpose of surveillance and FRT is to ensure the safety of citizens.[52]

Analysis

An analysis of these 20 countries' regulation of facial recognition technology reveals some countries are making more progress toward regulation than others. Table 1 outlines and summarizes the country-by-country analysis based on the qualitative data presented in the previous discussion. It also incorporates data on the level of democratic governance and more specific information on FRT laws. The table data reflect the presence of national laws or judicial decisions regarding FRT since 2016 and whether these mechanisms protect individual privacy from the government or private sector, prohibit real-time 1:N systems that can be used for mass surveillance—with limited exceptions, such as missing children—or prohibit the scraping of images on the internet to build the database.

The table also shows the presence of meaningful oversight of the use of FRT and whether the new laws provided substantial limitations and oversight of state surveillance and provided avenues of recourse for individuals. It includes data on how democratic the government is in each country, as assessed by Freedom House in its annual

48. "Venezuela: Freedom on the Net 2022 Country Report," Freedom House, 2022, https://freedomhouse.org/.

49. Paul Bischoff, "Facial Recognition Technology (FRT): Which Countries Use It? [100 Analyzed]," *Comparitech* [blog], January 24, 2022, https://www.comparitech.com/.

50. Bischoff.

51. Interception Of Communications Act (Chapter 11:20) [Zimbabwe], 2007, https://www.law.co.zw/; and "Surveillance and Privacy," MISA Zimbabwe, accessed April 24, 2024, https://zimbabwe.misa.org/.

52. Data Protection Act (Chapter 11:12) [Zimbabwe], 2021, https://www.dataguidance.com/; Ayang Macdonald, "Zimbabwe Govt Faces Criticism over Biometric Surveillance Project for New Smart City," BiometricUpdate.com, February 28, 2023, https://www.biometricupdate.com/; and "MISA Zimbabwe's Submission on the Surveillance Industry and Human Rights in Zimbabwe," UN Office of the High Commissioner for Human Rights, February 15, 2019, https://www.ohchr.org/.

Freedom in the World report. For the EU, the average democracy score of its members is presented in the table.[53]

Each factor—other than democratic governance—was assigned a score based on a yes/no answer; if the answer was "yes" then the country received a 1, and if the answer was "no" then it received a 0. The exception to this was the United States, which was the only country to receive a partial score (0.5) for presence of national laws on FRT because of the stringent laws in some parts of the country but the dearth of national laws overall. A higher score indicates that the country has taken more measures to protect individuals' privacy from potential abuses using FRT, whereas a lower score indicates fewer national laws to protect individuals' privacy from potential abuses.

53. *Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy* (Washington, DC: Freedom House, 2023), https://freedomhouse.org/.

Table 1. Facial recognition technology laws by country

Country	Democracy?	New national laws regarding privacy or FRT?	New laws protect individual privacy vis-à-vis the government?	New laws protect individual privacy vis-à-vis businesses?	New laws prohibit real-time FRT?	New laws prohibit 1:N systems?	Laws prohibit the scraping of images from the internet?	Evidence of laws that require meaningful oversight of the use of FRT?	Laws make state surveillance harder?	Total score
Argentina	0.85	1	0	0	0	0	0	0	0	1.85
Australia	0.95	0	0	0	0	0	0	0	0	0.95
Belarus	0.08	1	0	0	0	0	0	0	0	1.08
Belgium	0.96	1	1	1	0	0	0	0	1	4.96
Brazil	0.72	1	1	0	0	0	0	0	0	2.72
Canada	0.97	1	1	1	0	0	1	0	1	5.97
China	0.09	1	0	1	0	0	0	0	0	2.09
European Union	0.9	1	1	1	1	0	1	1	1	7.9
France	0.89	1	1	1	0	0	0	1	1	5.89
India	0.66	0	0	0	0	0	0	0	0	0.66
Israel	0.74	1	0	0	0	0	0	0	0	1.74
Japan	0.96	0	0	0	0	0	0	0	0	0.96
Myanmar	0.08	1	0	0	0	0	0	0	0	1.08
Russia	0.13	1	0	1	0	0	0	0	0	2.13
South Africa	0.79	1	0	0	0	0	0	0	0	1.79
South Korea	0.83	0	0	0	0	0	0	0	0	0.83
United Arab Emirates	0.18	1	0	0	0	0	0	0	0	1.18

Table 1 (*continued*)

Country	Democracy?	New national laws regarding privacy or FRT?	New laws protect individual privacy vis-à-vis the government?	New laws protect individual privacy vis-à-vis businesses?	New laws prohibit real-time FRT?	New laws prohibit 1:N systems?	Laws prohibit the scraping of images from the internet?	Evidence of laws that require meaningful oversight of the use of FRT?	Laws make state surveillance harder?	Total score
United Kingdom	0.91	1	0	0	0	0	0	1	1	3.91
United States	0.83	0.5	0.5	0	0	0	0	0	0	1.83
Venezuela	0.15	0	0	0	0	0	0	0	0	0.15
Zimbabwe	0.27	0	0	0	0	0	0	0	0	0.27

The data in table 1 capture a wide variety of legislative, policy, and legal positions around the world. Fifteen out of 20 countries had new legislation or legal rulings pertaining to the use of biometric and/or facial recognition technology. The major avenues for state regulation of FRT appear to be no legislation at all; legislation regulating private sector use of the technology; or legislation determining government use of the technology, including requiring citizens to use it in order to access state services, such as with Myanmar and Venezuela.[54]

Most countries have older data protection laws, but they are usually insufficient for protecting the biometric data used in FRT, thereby prompting the creation of new laws. New legislation grapples with at least five different areas of concern. First, regulating government use of FRT frequently addresses who can use this technology, under what circumstances it can be deployed, and what type of capabilities are permissible. For instance, 1:1 FRT has very different implications than 1:N, and the implications of real-time FRT surveillance differ from those concerning FRT deployed on recorded or delayed surveillance recordings.

Second, the legislation typically addresses the extent of government use of the technology and may establish oversight mechanisms and systems of redress; however, the effectiveness and meaningfulness of this oversight varies significantly in each country. Third, how the database of images is constructed is an issue for legislative concern. Some FRT companies scrape images from the internet and social media to create the largest possible database but cannot gain the consent of the people whose images are included. Others construct databases of known persons of interest and limit searches to just these individuals; however, it is important to have oversight and clear criteria for adding individuals to the database to prevent misuse and abuse.

Fourth, storage and protection of databases of biometric data is also an issue for legislation so that the data cannot be stolen or illegally manipulated. This is particularly important as the data may be stored for decades. Fifth, legislation varies in addressing the scope for FRT use in society. Many existing laws do not address potential for public-private partnerships between governments, particularly law enforcement. Moreover, private security companies may own and operate cameras and provide data to the government. Many laws are not specific enough on the issue of scope.

There are interesting trends in the differences in legislation between democratic and nondemocratic countries. The countries that have passed legislation to protect privacy rights and human rights have all been democracies. The EU scored the highest in this study, followed by France and Canada; these democratic entities have prioritized protection of privacy and human rights and enacted laws to support them.

Yet some of the countries with the lowest scores—including Australia and the United States—are democracies that have not yet passed legislation to regulate FRT. The absence of laws creates a legal void similar to what is seen in nondemocratic countries that have chosen not to regulate FRT. Authoritarian or nondemocratic

54. "Venezuela: Freedom on the Net"; and Pascu, "Myanmar."

regimes have tended to pass legislation that protects the regimes' interests in using FRT and stymies legal challenges to it.

The lowest scoring countries were Argentina, Australia, India, Israel, Japan, Myanmar, South Africa, South Korea, UAE, the United States, Venezuela, and Zimbabwe. There are several reasons that these countries scored so low, particularly among democracies. For some countries, cultures of privacy focus on communalism instead of individuals, thus diminishing the expectation of protection of individual privacy rights. There may also be economic goals of becoming industry leaders or pioneers in the uses of FRT, such as with Japan's AI FRT drone delivery system.[55] For others, the challenges of passing national legislation in large, diverse countries present significant difficulty and may require more time or a piecemeal approach across different jurisdictions.

In Australia and the United States, the citizenry are having robust debates over FRT and legislative efforts underway to regulate its use, but national governments have yet to pass legislation on the issue.[56] In the United States, several cities and states have passed legislation that curtails or bans the use of FRT, but there is no federal law, and the majority of the country is not covered by any particular legislation.[57] For some countries, such as Israel, the presence of ongoing conflict and national security concerns appears to outweigh the protection of privacy rights.[58] And finally, some regimes are more authoritarian in nature and do not seek to protect their citizens' privacy rights in a robust or meaningful way.

Recommendations

The use of FRT and legislation governing it vary widely in intent and implementation around the world. Facial recognition technology laws are built upon existing norms of privacy and human rights, but they also provide an opportunity for each country to decide if it will continue on the same trajectory or diverge onto a different path. Nearly every country examined had evidence of popular protest or legal challenges against the use of FRT systems, indicating that regardless of country or legislative framework, people want their privacy and human rights protected.

This research found there is not yet a meaningful distinction between the rate of legislative actions of democracies and nondemocracies. Some democracies have adopted robust laws to govern this technology, but many others have not yet—and some do not appear to be likely to do so anytime soon. When democracies have passed legislation, they have acted to protect their citizens' privacy and human rights and make

55. McConvey, "Trains, Drones and Robotic Feels."

56. Field, "Facial Recognition."

57. Skye Witley and Andrea Vittorio, "Facial Recognition Software Is Everywhere, with Few Legal Limits," Bloomberg Law, April 27, 2023, https://news.bloomberglaw.com/; and Ryan-Mosely, "Movement to Limit."

58. "Ministers to Approve Bill Legalizing Police Use of Facial Recognition Cameras," *Times of Israel*, September 23, 2023, https://www.timesofisrael.com/; and Elizabeth Swoskin, "Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank," *Washington Post*, November 8, 2021, https://www.washingtonpost.com/.

government surveillance more difficult or require greater oversight. Europe appears to have the greatest momentum for passing legislation to protect individuals' rights, with the passage of the new EU legislation and preexisting laws in France and Belgium. Canada and Australia have also taken significant steps in this direction.

In every country examined, FRT was implemented before legislation and policy were developed to regulate its use. Prior legislation that regulated collection of data and privacy was typically insufficient for the collection of biometric data and lacked the legal oversight mechanisms many countries sought. Concerns about privacy and human rights have been raised in almost every country in this study. Yet some have acted swiftly to address concerns, while others have moved rapidly to embrace the technology and expand its use. It may be too early to tell how FRT will impact global norms for privacy. It is clear, however, that countries are embracing FRT in different ways, and individual countries are intentionally choosing different approaches to regulating it. These approaches likely reflect economic goals as well as norms and expectations of privacy and government regulation.

These findings are relevant for senior military and civilian leaders because they provide an opportunity for leadership to advance US values and soft power. Specifically, the United States has a chance to promote global standards and norms for the responsible use of FRT consistent with its interests. It could strengthen alliances and partnerships by collaborating on legal and policy positions consistent with its closest partners. The United States could work toward creating a regional or global norm regarding the balance of technological innovation and fundamental rights.

Facial recognition technology also affects US military and civilian personnel stationed overseas and private US citizens traveling abroad. The lack of international regulation or consensus around FRT raises questions about how images and identities of US military and civilian personnel overseas can be protected. The US military can add protections for such US personnel by setting expectations and creating dialogue for regulations concerning the use of FRT. These expectations could be clarified and codified in US laws or agreed to in international forums. The United States should seize the opportunity to determine what legal and normative responsibilities and recourse could be established to protect US personnel and advance national security.

As rapid technological innovation in the field of biometric surveillance proceeds, policymakers and legislators must be aware of the implications for human rights and privacy. As governments and companies invest in developing and implementing this technology to improve safety and security, they should also invest in safeguarding the human rights and privacy of citizens. Such laws and protections will not only affect citizens but will also determine the emergence of new norms in international law applicable to cyberspace and technology. **Æ**

ENERGY WEB DOMINANCE

A Proposal for a Fourth Offset Strategy

PAUL CALHOUN

America's military advantage in power projection has eroded significantly due to adversarial anti-access/area-denial (A2/AD) strategies. A multidomain, networked peer adversary combat environment has emerged from these A2/AD strategies, threatening longstanding military trends. Recognizing that energy is a fundamental element in warfare, researchers at the Defense Advanced Research Project Agency have developed an energy web dominance portfolio to explore innovative methods of optimizing energy distribution to create a more dynamic and resilient network. This energy web dominance framework provides a novel perspective on the fundamental character of warfare, revealing new opportunities for optimizing military effects delivery leveraging wireless energy distribution technology breakthroughs.

Energy and information are fundamental currencies in the battlespace. Since the 1700s, there has been a revolution in information transport, transforming its flow from physical point-to-point transfers such as paper letters into a more resilient multipath network, such as data through the World Wide Web. More recently, ubiquitous wireless communication has dramatically transformed the flexibility and utility of information distribution.

Recent research pioneered by the Defense Advanced Research Projects Agency (DARPA) suggests a similar revolution may be imminent in the energy domain. Causing or delivering military effects costs energy. Wireless power transfer capabilities being developed as part of DARPA's energy web dominance (EWD) portfolio provide one compelling candidate breakthrough technology which may transform the battlespace, providing the next significant technology offset in warfare.

This article introduces energy web dominance as an analysis framework that recognizes the centrality of energy in the battlespace. This framework provides strategic and tactical insight into optimizing military effects delivery considering energy generation, storage, and distribution. The context for this optimization is the networked,

Colonel Paul Calhoun, USAF, a experimental test pilot supporting the US Air Force Test Center and former Defense Advanced Research Projects Agency (DARPA) program manager, holds a master of science in aeronautics and astronautics from the Massachusetts Institute of Technology, a master of science in flight test engineering from the US Air Force Test Pilot School, and a master of science in national resource strategy from The Eisenhower School for National Security and Resource Strategy.

multidomain sense-and-kill capabilities developed by adversarial nations that the author and team members refer to as the peer adversary combat environment or PACE.

In the 1980s and 1990s, the United States developed stealth- and precision-guided weapons technologies as part of the Second Offset Strategy to defeat the former Soviet Union's legacy integrated air defense systems (IADS), which primarily used ground radars for sensing and centralized command and control (C2) to direct responses. Desert Storm provided validation of the Second Offset's effectiveness against a legacy IADS approach. Seeing that the traditional IADS approach was ineffective against US tactics and force structures, adversarial nations developed anti-access/area-denial (A2/AD) strategies as a counter.[1]

The peer adversary combat environment, then, is the instantiation of A2/AD strategies. Today, this environment is no longer just a strategic framework but rather a physical environment where US forces must survive, operate, and dominate to achieve military effectiveness, and countering this environment requires a new approach. The EWD framework provides a novel perspective on the fundamental character of warfare, revealing new metrics for optimizing the delivery of military effects.

Background

Significantly, the current US military force structure remains rooted in Second Offset weapons and platforms even though the peer adversary combat environment was specifically developed to counter those systems. Second Offset–era trends have led to high-cost, high-capability manned platforms, such as B-2s and aircraft carriers. In the modern combat environment, incremental increases in survivability are prohibitively expensive, leading to limited quantities of these assets. Losing even one of the United States' 19 B-2s or 11 aircraft carriers would have a significant impact on US military capability. This is in addition to the raw cost. It is feasible in the peer adversary combat environment that a $1 million missile could destroy a $2.2 billion B-2, magnifying the cost imposition for the United States and leading to a losing resource race against a peer adversary.[2]

In 2016, recognizing a new strategy was imperative, then Under Secretary of Defense Robert Work proposed a Third Offset Strategy in policy speeches. In this offset strategy, he stated networked human and machine teams in large quantities would be able to overwhelm A2/AD environments and sustain the United States' ability to project military power.[3] A key element of his approach is resilient, multipath information networks adaptively concentrating information for decision-making and command and control. A remaining challenge is developing platforms that can be employed in large quantities at

1. Rebecca Grant, "The Second Offset," *Air & Space Forces Magazine*, June 24, 2016, https://www.airandspaceforces.com/.

2. Jacopo Prisco, "B-2 Spirit: The $2 Billion Flying Wing," CNN, January 29, 2020, https://www.cnn.com/.

3. Ian Livingston, "Technology and the 'Third Offset' Foster Innovation for the Force of the Future," Brookings, December 9, 2016, https://www.brookings.edu/.

long ranges. Insights from the information revolution in Work's Third Offset applied to the energy distribution are the foundation of the DARPA EWD portfolio's presentation of a Fourth Offset Strategy to enable long-range platforms in overwhelming quantities.

Currently, if a platform requires long-range, endurance, or significant weapons-delivery capability, it must be physically large. Platforms are designed as containers that carry the energy needed to complete a mission in the form of liquid fuels, batteries, or chemical explosives. These large platforms are expensive and are therefore purchased in limited quantities. Some research, such as DARPA's Gremlins and LongShot programs, has looked at providing large quantities over long ranges by using large hosts and with small surrogate aircraft.[4] Other research looked at aggregating and disaggregating small platforms to achieve the benefits of efficiency or resilience depending on the threat. These programs suggest such architectures are effective and feasible with current technology but also highlight fundamental limitations in energy storage.

Second Offset technology has logically led to a platform-centric force structure due to assumptions about information and energy. Decision-making was accomplished at the platform level by human operators putting a lower limit on platform size and driving survivability requirements to preserve human life. Energy is also stored at the platform level, coupling performance to volume.

Following Norman Augustine's 16th "law," as platform capability has increased, there has been an exponential increase in costs: "In the year 2054, the entire defense budget will purchase just one tactical aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day."[5]

Though Augustine published his laws as satire, the data has validated the underlying trend: in static or linearly increasing budget environments, the number of platforms purchased has steadily decreased.[6] As the number of platforms decreases, the need for individual platform survivability increases, which further accelerates the trend. This is sustainable if survivability can be improved commensurate to the cost increases and if enough platforms still exist to provide flexibility.

Yet threats in the peer adversary combat environment have changed significantly, making further incremental increases in survivability prohibitively expensive. At the same time, technological opportunities have also changed, challenging the underlying assumptions that led to the current force structure. Advances in autonomy and networked information allow for distributed C2 so that a human operator is not necessary on many platforms. A wireless energy web could provide a radical alternative by allowing platforms to act as conduits rather than containers.

---

4. See Paul Calhoun, "DARPA Emerging Technologies," *Strategic Studies Quarterly* 10, no. 3 (Fall 2016), https://www.airuniversity.af.edu/; "Gremlins," DARPA (Defense Advanced Research Projects Agency), accessed April 11, 2024, https://www.darpa.mil/; and John Casey, "LongShot," DARPA, accessed April 11, 2024, https://www.darpa.mil/.

5. Norman R. Augustine, *Augustine's Laws* (Boca Raton, FL: United Press International, May 24, 1986).

6. Calhoun, "DARPA Emerging Technologies."

The amount of energy a platform could carry would not be a performance constraint; rather, the energy that flows through the network would enable capabilities. Offboarding energy storage and generation would decouple platform size from performance. Of note, many military missions require more energy than is available by only harvesting or scavenging energy—for example through photovoltaic solar cells—which drives the need to externally augment energy inputs. Wireless energy beaming (WEB) technologies in development at DARPA coupled with distributed C2 would enable small, inexpensive platforms to have significant capabilities, such as practically unlimited range, indefinite persistence, and arbitrary amounts of power available for their payloads or weapons.

In contrast to the Second Offset's platform-centric approach, the Third and Fourth Offsets encourage a network centric-approach where capability is scalable by adjusting the quantity of platform nodes employed in any given scenario. The network, not the platform, becomes the nexus of capability. Individual nodes are attritable and thus can be dramatically less expensive, since the strategy shifts to overwhelming with quantity rather than exquisite survivability. As an example, a B-2 has a fixed capability whether it is employed against a highly defended target or an undefended target. Since the most constraining cases are rare, in most employment scenarios the B-2 has excess capability, which means from a resource standpoint, delivering that effect costs more than necessary.

Scaling capability through quantity considers that the simplest targets are vulnerable to a single wireless energy beaming platform. When facing more complex targets, more WEB platforms are used to overwhelm defenses. As a result, capabilities are scalable across a range of scenarios optimizing resource allocations.

There is an ongoing, robust debate about the correct mix of high-technology and low-technology platforms. Assuming a solitary platform type can scale in capabilities across all scenarios is overly simplistic, but such an assumption provides useful guidelines, implying that WEB technologies provide advantages across the spectrum of threat environments. Relying on inefficient capabilities overmatch as done now may be acceptable against a resource-poor adversary. Against an economic peer, however, sustained operations rely on efficient effects delivery.

Energy in the Battlespace

The revolution in platform capability is an important element of implementing WEB, but understanding the impact of energy flows in the battlespace is actually even more fundamental. Throughout history, warfare has favored the combatant who can effectively maneuver and resupply their forces. As General John J. Pershing once said, "Infantry wins battles, logistics wins wars."[7] Fundamentally, logistics is about

7. Jason Lee, "New Logistics Commander Praises 'Complex,' 'Important' Work at Hill Air Force Base," KSL.com, August 31, 2017, https://www.ksl.com/.

transporting the capability to cause military effects, and energy is the coin of the realm. The form of that energy has evolved over time.

During the Roman Empire this energy came in the form of food for horses and men converted to military effects through physical action. In the Civil War, coal for trains and gunpowder for muskets were the preferred energy storage mediums. In the modern era, chemical energy is stored in explosive warheads and liquid hydrocarbon fuels. Energy transport breakthroughs such as Roman roads, railroads, mechanized warfare, and air-refueling tankers that more rapidly and resiliently move energy through the battlespace have provided decisive military advantages. Indeed, contemporary American military dominance has been built upon asymmetric advantages in air refueling tankers and a nuclear navy, allowing the United States to position mobile energy wells forward in the battlespace.

Noting this advantage, adversary nations have specifically developed weapons to counter air refueling tankers and carrier strike groups as a core tenet of their A2/AD strategy from which the peer adversary combat environment has emerged. While tankers and nuclear carriers have provided that decisive advantage in the past, maintaining energy web dominance in the future will require a new approach.

To paraphrase Antoine Henri Jomini, the science of war is focusing energy on decisive points.[8] The corollary art of war, which is analyzing the battlespace to determine where those decisive points exist, can be considered an information domain endeavor. In John Boyd's now canonical observe, orient, decide, act (OODA) loop, there are information and energy domain elements for each iteration.[9] Observation requires some sensor with physical presence that requires energy to persist in its given environment. Orienting is an information domain function consisting of sifting data for sense making then delivering that information to a decision hub. Deciding is an information domain activity to determine an optimal course of action based on available data. Acting requires an energy transaction to both cause and deliver the intended military effect.

Since the early 2000s, net-centric warfare has revolutionized information flows, including significant work over the last decade in developing artificial intelligence/machine learning tools to enhance decision-making.[10] Energy logistics, on the other hand, have remained relatively static since the advent of mechanized warfare, which still relies primarily on mass-based transfers of liquid fuels that are slow, linear, and vulnerable. Energy web dominance considers end-to-end effects delivery with no clear boundary between logistics and tactics. Instead, there is a continuum where the optimal network adjusts between efficiency and resilience, depending on the existing threat. Generally, networks with fewer nodes are more efficient while networks with more redundant nodes are more resilient.

8. Antoine Henri Jomini, *The Art of War* (St. Paul, MN: Wilder Publications, 2008).

9. John R. Boyd, *A Discourse on Winning and Losing*, ed. and comp. Grant T. Hammond (Maxwell AFB, AL: Air University Press, 2018).

10. Arthur K. Cebrowski and John H. Garska, "Network-Centric Warfare – Its Origin and Future," *US Naval Institute Proceedings* 124, no. 1 (January 1998), https://www.usni.org/.

Imagine the battlespace populated by energy nodes. In the all-domain battlespace of today, a tanker is a node, an aircraft carrier is a node, and an F-22 is a node. Each participant consumes and delivers energy as needed to achieve military effects. Imagining the battlespace as a network of energy nodes provides a new optimization surface for quantifying effects delivery versus costs. If these nodes are connected by physically transferring energy via liquid fuel, they accept limitations in flexibility since such a transaction is predictable and slow. As technological advances create nodes that flow energy wirelessly through the electromagnetic spectrum, combatants will see considerable increases in speed and flexibility.

Within the current energy logistics construct, chemical energy stored in a warhead might be used to destroy an enemy radar site. To deliver that military effect from the factory where that warhead was made, it would be placed on a ship to cross the ocean, consuming fuel as energy along the way for delivery to a forward staging area. From there it might be loaded on an F-22, likely with insufficient energy reserves to deliver that effect the full distance, requiring fuel from a tanker en route. If any part of this chain of subsequent energy transactions is broken, the military effect would not be delivered.

The platforms associated with these energy transactions—tanker ships and air refueling aircraft—are large, expensive, and difficult to replace. Furthermore, the fixed infrastructure supporting these transactions, such as ports and runways, takes weeks or months to reconstitute if destroyed. As a result, energy logistics today are slow, brittle, and do not recover quickly from disruptions.

Consider instead a web of wireless energy nodes. These nodes might be unmanned aerial vehicles (UAVs), ships, manned aircraft, preplaced hidden ground stations, space assets, undersea assets, or any number of multidomain options. To deliver an effect, power generated from an aircraft carrier might be delivered to a satellite across thousands of miles to another satellite and then routed through a network of UAVs to focus directed microwaves at the radar site to destroy it. In this scenario, if any single node of the web were disrupted, other nodes would be used to deliver the energy.

This wireless energy web would be constructed with built-in multipath resilience, so it degrades gracefully when under attack. These nodes can be both small and persistent, because they are being constantly recharged by the energy web. If a $1 million missile is needed to destroy a $50,000 energy node UAV that could be immediately replaced by dozens of others, an adversary is faced with a cost and resources dilemma. Rerouting to another multipath option can be accomplished in seconds, and full reconstitution by replacing missing nodes can be accomplished in hours or days.

Such a network is robust, resilient, and can be rapidly repaired. Additionally, in this wireless energy web, transfers are happening at the speed of light, which for reference is roughly Mach 1 million. The United States has invested heavily in hypersonic weapons that are orders of magnitude slower. While hypersonics do serve an important function, the potential of delivering speed-of-light effects at scale provides a compelling alternative. Dynamic strike flexibility, where the focus of an attack can shift thousands of miles in less than a second, revolutionizes the concept of maneuver warfare, making it

nearly impossible for an adversary to position and maneuver reaction forces to counter all of the potential attack vectors.

Energy Web Dominance Framework

The energy web dominance framework is not a new technology set but rather a recognition of a fundamental aspect of warfare. Within this framework, DARPA has identified breakthrough distribution technologies as an area ripe for disruption. There are already considerable investments in developing new energy storage and generation technologies, and DARPA seeks out areas where focused investments can have dramatic impact, such as wireless energy beaming. The EWD framework does not assert that wireless power transfer is the right solution for all energy scenarios. Rather, it seeks to optimize energy flows for speed and resilience.

Indeed, in some scenarios the energy density required cannot be supplied wirelessly. Supersonic aircraft, for example, are relatively small and require more energy than can likely be provided wirelessly without significant transmission and cooling challenges. Wireless energy beaming is an important addition to the technology toolset, but this does not mean continued progress in other areas of energy generation, storage, and distribution is no longer relevant. Fundamentally, EWD will look at advances in all areas and continue to optimize the energy network for effects delivery. If, for example, batteries were developed with ten thousand times the current energy storage density, wireless power beaming would become a less important part of the overall energy optimization.

This framework does suggest a new focus on the network as the basis of maneuver rather than platforms, which is greatly enhanced by beaming energy wirelessly. This allows effects delivery in many cases through nodes that do not require much energy instead of fast platforms. Instead of energy hungry, expensive, supersonic aircraft delivering effects, think instead of relatively slow-moving, energy-efficient, and inexpensive high-altitude nodes acting as the conduits through which the speed-of-light effects are delivered. So while delivered energy density does remain a challenge for some platforms using wireless power transfer technologies, the EWD framework itself provides potential solutions.

The peer adversary combat environment is multidomain and mesh networked. The *National Defense Strategy* has identified China as the pacing threat, and thus the Chinese peer adversary combat environment is the primary context inspiring DARPA's EWD portfolio.[11] Defeating a single sensor or shooter in this environment is insufficient to creating sustained advantage. As former Commander of US and International Security Assistance Forces Afghanistan and Joint Special Operations Command General Stanley A. McChrystal often said, "To beat a network you need a network."[12] While the context

11. Lloyd J. Austin III, *National Defense Strategy of the United States of America including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Office of the Secretary of Defense, October 2022), https://media.defense.gov/.

12. Stanley McChrystal, "It Takes a Network," *Foreign Policy*, February 21, 2011, https://foreignpolicy.com/.

of McChrystal's proclamation was focused on human networks, it reflects the deeper truth that building resilient and dynamic connections across a network provides a competitive advantage.

Evolution in military technologies increasingly makes all warfare reliant on networks. The energy web dominance framework significantly expands the scope of network capabilities by also considering energy to holistically look at the pathway from energy generation through decision-making to effects delivery. With history as a guide, it is clear that leveraging energy effectively in the battlespace is at the heart of operational art.[13] Exploring new energy technologies is vital to modernizing the US military.

Wireless Power Transfer Technologies 101

An analysis of the current state of the art in wireless power transfer coupled with targeted DARPA investment reveals the military utility of wireless power transfer. The concept of wireless power transmission gained popularity with Nikola Tesla and the electrification of civil society. In Tesla's time, the concept was ahead of the technical status quo. Today, however, emerging technologies, including robust high-energy lasers, high-efficiency monochromatic bandgap matched photovoltaics, and dynamic radio frequency (RF) beam forming that includes distributed coherent techniques, provide the fundamentals required to create effective wireless power beaming links. DARPA's novel energy web dominance efforts aim to unite these technologies in a multipath network to overwhelmingly counter the peer adversary combat environment.

Certain fundamental wireless power technologies serve as the building blocks for the wireless energy web, including close- and long-range links.

Close-Range Links: Field-Based Wireless Power Transfer

Wireless power transfer over relatively short ranges can be accomplished using electromagnetic field effects. Induction uses changing magnetic fields to create currents in conductive materials. Field-based power transfer only draws power from the host when there is a recipient present. This allows for very high-power transmission efficiencies up to 99 percent.[14] Standard inductive coupling is effective for ranges equivalent to the inductive coil's diameter.[15] A familiar example is an iPhone charging pad. While useful in some contexts, however, standard inductive coupling lacks the range to provide much utility for an extended wireless energy web.

---

13. Moshe Kress, *Operational Logistics: The Art and Science of Sustaining Military Operations* (New York: Springer, 2002).

14. Editors of *Encyclopedia Britannica*, "Electromagnetic Induction (Physics)," *Britannica*, last updated February 2, 2024, https://www.britannica.com/.

15. John Macharia, "Wireless Inductive Charging for Low Power Devices" (thesis, Helsinki Metropolia University of Applied Sciences, January 31, 2017), 6, https://www.theseus.fi/.

One subset of induction enhances range through tightly coupled magnetic resonance. When fitted with a high-quality factor resonator, a device that responds specifically to a particular frequency, the effective range of near-field power transfer can be extended to about 10 times the aperture diameter. Quality factor for resonators is a measure of the precision of the frequency response.[16] In laboratory settings, this technique has been demonstrated out to around 10 feet, effectively.[17]

Using larger antennas and higher-quality resonators, it would be possible to extend this out to dozens of feet. At these ranges, air recharge from an airborne host or persistent power to hovering UAVs from a ground station is a viable application. Likewise, any electric device such as a radio or computer could draw power from a local node, allowing it to operate indefinitely without plugging into an existing grid. There are a number of commercially available products that provide inductive wireless charging solutions.[18]

Long-Range Links: Wireless Energy Beaming

Power beaming sounds exotic, but it actually involves the same physics as that involved in wireless communication. A power source is converted to a propagating wave, typically electromagnetic, sent through free space, collected through an aperture, and converted back to electricity. In a cellphone, that electricity is used as a signal that encodes voice or data. For power beaming, that converted electricity is used directly for power. Point-to-point power beaming has been successfully demonstrated using a variety of transfer methods. Laser and microwave power beaming are the most mature technologies. DARPA has also explored acoustic power beaming for underwater applications. The demos to date serve as excellent proof-of-concept benchmarks but also highlight some of the ongoing challenges.[19]

First, many previous demos were custom built to work with a particular transmit-and-receive pair and generally were not suitable for use in a larger scalable network. Second, conversion efficiencies remain a challenge. In a multihop network, converting from a propagating wave back to electricity back to a propagating wave at each node quickly accrues unacceptable losses. Each one of those conversions is relatively inefficient and multiplying them across a chain is impractical. DARPA has identified effective power-beaming relays as a critical element for overcoming these challenges to creating a practical power-beaming network.

The DARPA Persistent Optical Wireless Energy Relay (POWER) program seeks to make long-distance networked optical power transfer practical by developing effective

16. Estill I. Green, "The Story of Q," *American Scientist* 43, no. 4 (October 1955), https://www.jstor.org/.

17. Macharia, "Wireless Inductive Charging," 6.

18. "Wireless Power Network," Global Energy Transmission, 2024, accessed April 12, 2024, https://getcorp.com/; and "WITRICITY WIRELESS EV CHARGING: The Cure for Charge Anxiety," WiTricity, accessed June 14, 2024, https://witricity.com/.

19. Paul Calhoun, "DARPA Energy Web Dominance Summit Introduction," July 6, 2023, uploaded by DARPATV, YouTube video, October 17, 2023, 45:05, https://www.youtube.com/.

optical energy relays (fig. 1). In this system, a ground-based laser transmitter relays a power beam to a high-altitude relay that then relays that energy to a distant aircraft, which relays the power beam to a receiving station on the ground. An effective optical relay must efficiently redirect energy without conversions, correct wavefront aberrations to maintain a tight beam for long range, and selectively collect some of the energy to power itself.[20]

Figure 1. DARPA's Persistent Optical Wireless Energy Relay Program (POWER)[21]

For optical power beaming, transmission through the lower, thick, and turbulent atmosphere is impractical over long distances due to beam spread and attenuation. High-altitude transmission is quite effective, but having a high-energy laser at high altitudes presents payload weight and cooling challenges. Effective relays allow the combination of ground-based lasers with a high-altitude transmission network, optimizing energy generation and transmission across the system.[22] DARPA envisions this high-altitude optical layer providing the long-range, high-throughput backbone for the wireless energy web.[23]

Shorter-range—tens of meters to several kilometers—distribution to many devices may be most effectively accomplished using RF power beaming. This is more effective through weather and can be easier to operate safely around objects and people. When considering optical versus RF power beaming, it is helpful to understand a bit of the tradespace between wavelength, range, efficiency, and size of the transmit-and-receive apertures.

20. "Power," DARPA, accessed April 12, 2024, https://www.darpa.mil/; and "Persistent Optical Wireless Energy Relay (POWER) Broad Agency Announcement," SAM.gov, accessed April 12, 2024, https://sam.gov/.
21. "Power."
22. "Wireless Energy Relay."
23. "Wireless Energy Relay."

Both RF and optical power beaming rely on transmitting electromagnetic propagating waves. For the most efficient power beaming, the beam size at the desired range should be the same size or smaller than the receiving aperture so that all of the energy is captured. As these waves travel through free space, they generally expand through diffraction, so that the farther away the receiver is the larger the spot size.[24] Think of how a flashlight behaves when shining it across a room. As it turns out, the spot size is impacted most significantly by wavelength and the size of the transmit aperture. Larger apertures create smaller beams and spot sizes while smaller wavelengths produce smaller beams and spot sizes.

Optical beams have much smaller wavelengths than RF beams, which means they can have smaller spot sizes. A smaller spot size can mean a smaller aperture at a set range, or it can mean that for a particular aperture size efficient transmission is possible at larger ranges. For electromagnetic waves, frequency and wavelength are inversely related, so a higher frequency has a smaller wavelength. Generally, since RF waves have much larger wavelengths (lower frequencies) than optical waves, efficient transmission over an equal distance requires much larger apertures.[25]

In 1975, the Jet Propulsion Laboratory, sponsored by the National Aeronautics and Space Administration (NASA), transmitted 34 kilowatts at a frequency of 2.45 gigahertz (GHz) over a distance of 1.5 kilometers (km) with 82 percent transmission efficiency, setting a still-standing benchmark in throughput.[26] At this same frequency, if the receive antenna was moved out to 10 km, an antenna area of 1,224 square meters (sq m) would be needed to capture 60 percent of the incoming wave.[27]

Higher frequencies (smaller wavelengths) allow for smaller antennas. For example, at 100 GHz at that same 10 km, 60 percent of the wave is captured with a 30 sq m antenna.[28] This is further complicated by variable atmospheric effects dependent on frequency. Generally, in the RF portion of the spectrum, lower frequencies have less absorption in the atmosphere and can penetrate clouds. While this trend is true in reality across the spectrum, there are known transmission windows with less absorption that are useful for power beaming or long-distance wireless communications.[29]

Notably in the context of power beaming, there is a very efficient atmospheric transmission window around optical frequencies, which incidentally helps to explain why human vision detects electromagnetic waves in this portion of the spectrum. RF

24. Jacob Gavan and Saad Tapuchi, "Microwave Wireless-Power Transmission to High-Altitude-Platform Systems," *URSI Radio Science Bulletin* 2010, no. 334 (September 2010): 30, https://ieeexplore.ieee.org/.

25. Shaopeng Wan and Kama Huang, "Methods for Improving the Transmission-Conversion Efficiency from Transmitting Antenna to Rectenna Array in Microwave Power Transmission," in *IEEE Antennas and Wireless Propagation Letters* 17, no. 4 (2018): 540, https://ieeexplore.ieee.org/.

26. "1975 NASA JPL Goldstone Demonstration of Wireless Power Transmission," Citizens for Space Based Solar Power, uploaded by Rob Mahan, March 11, 2008, YouTube video, 2:15, https://www.youtube.com/.

27. Gavan and Tapuchi, "Microwave Wireless-Power Transmission," 30.

28. Gavan and Tapuchi, 31.

29. "The Atmospheric Window," National Oceanographic and Atmospheric Administration, last updated April 10, 2023, https://noaa.gov/.

power transfer has proven effective, but there are considerable trades to be made between aperture sizes, frequency, and efficiency for implementation within a networked energy framework.

Active electronically scanned arrays have brought considerable flexibility to radio frequency beamforming. Using a single transmitter with signals split between an array of emitters, they phase shift coherent signals to each emitter to create concentrated beams of RF signal using constructive and destructive interference. As discussed in the previous paragraph, beam width/spot size and transmit aperture size are inversely related. A larger transmit aperture produces a smaller beam which supports a smaller receive aperture.

Coherent beamforming using distributed arrays allows multiple separate transmitters to appear electromagnetically like one large aperture. Thus, less expensive distributed systems can achieve these same beam widths as a single large aperture and do so more resiliently since they are no longer a single point of failure system. The primary technological challenge is ensuring the waves are synchronized, since they are now generated by multiple transmitters and are thus not coherent from the outset. Several techniques have proven effective in laboratory testing.[30] Further research will test if this can be employed reliably in operational environments including dynamic tracking of moving platforms.

Distributed arrays provide two significant advantages for wireless power transfer: (1) concentrated beamforming with significant power gain, and (2) lower power required per transmitter, which allows for small, low-cost platforms. Distributed arrays have a power gain that scales by the square of the number of nodes in the array. Intuitively one might expect a linear scaling, where four transmitters' signals combine for four times the power at the receiver. Linear scaling is in fact the case for noncoherent transmission. Yet, as discussed above, with coherent transmission, the area of the distributed arrays combines, giving an added transmission gain due to the smaller beam width and spot size.

As a result, for an array with eight nodes, the received power is 64 times greater than what would have been received from a single transmitter node.[31] This allows each node to operate at lower power levels, which supports inexpensive systems. Scaling up to potentially dozens of nodes in an array, the gain becomes even more significant. Additionally, systems with many transmitting nodes are resilient when compared to a single transmitter. If one or more transmitters fail in a multinode system, the power transfer decreases gradually.

---

30. Raguraman Mudumbai et al., "Distributed Transmit Beamforming Using Feedback Control," *IEEE Transmission Information Theory* 56, no. 1 (2010), https://doi.org/; Robert. D. Preuss and D. Richard Brown III, "Two-Way Synchronization for Coordinated Multicell Retrodirective Downlink Beamforming," *IEEE Transmission Signal Processing* 59, no. 11 (2011), https://doi.org; and Jeffrey A. Nanzer et al., "A Review of Microwave Wireless Techniques for Human Presence Detection and Classification," *IEEE Transactions on Microwave Theory and Techniques* 65, no. 5 (2017), https://doi.org/.

31. Jeffrey A. Nanzer, interview by the author, and PowerPoint presentation, January 5, 2020.

Recently a DARPA-funded demonstration validated graceful degradation in a distributed coherent beam forming a wireless energy mesh network (fig. 2).[32] Figure 2 represents concept artwork of a real-world demonstration showing a UAV being charged by four distributed RF transmitters. The UAV is flying directly above the transmitters, which have RF waves converging on a receiving aperture on the UAV. The UAV and the transmitter are depicted in a hanger representative of the actual hanger at NASA Ames in the Silicon Valley, where this test took place. Arguably, coherent beamforming using distributed arrays is a critical technology that will enable distributed low-power, low-cost nodes to effectively concentrate effects within the energy web.

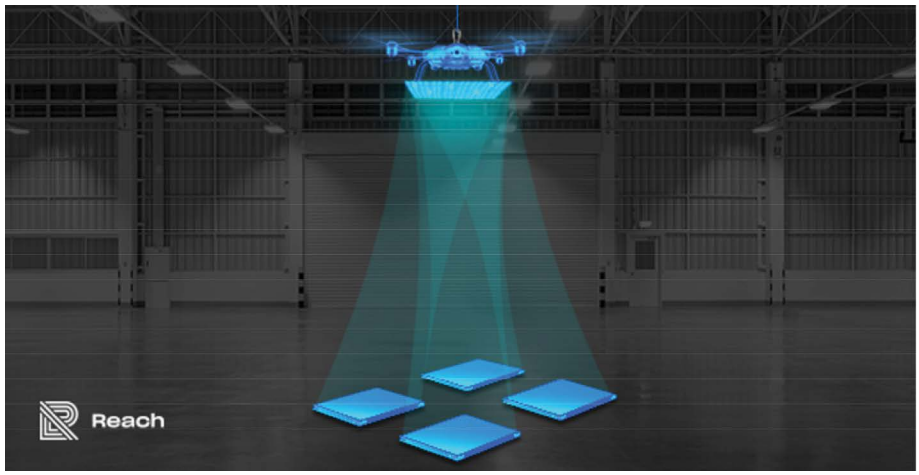

Figure 2. UAV recharged in flight using distributed coherent RF transmitters

Network Effects

The future energy web is envisioned as an expansive network where energy sources and consumers can partake of the network with proper authentications. This will demand careful attention to establish open but secure network protocols. This network should be able to harness multiple transfer modalities depending on environmental conditions and will require new C2 concepts to optimally position nodes based on expected demand.

This open architecture may enable new, exotic energy sources such as space-based solar, moon-based solar, the harnessing of deep ocean waves, or the parasitic stealing of adversary energy.[33] Within the energy web dominance framework one could imagine a

32. A. Porteus, "Reach Enables Wireless Power Mesh Networking for In-flight Drone Charging," Reach, May 23, 2024, https://reachpower.com/.

33. Daniel Wood, "Space-Based Solar Power," Energy.gov, accessed March 22, 2020, https://www.energy.gov/; and Dave Criswell, "Lunar Solar Power (LSP) System: Practical Means to Power Sustainable Prosperity," Search and Discovery Article #70070 (2009), 17, https://www.searchanddiscovery.com/.

stealthy UAV perching on enemy power lines and beaming that power to incoming American forces to use against that adversary.

Moon-based solar is a particularly revolutionary concept that proposes using self-replicating robots to transform the moon's silicon-rich soil into solar cells. In essence, the moon would become a giant power-generating solar farm, dramatically changing energy dependence on traditional sources.[34] Deep ocean waves can generate significant amounts of energy, but building fixed infrastructure out to the deep ocean is impractical.[35] The key to unlocking these future sources is building a network that can effectively distribute energy over long ranges.

Long before the wireless energy web transforms civil energy infrastructure, it will provide a compelling advantage for military forces. Before a technology can replace its predecessor, it must prove that it is significantly better to justify replacement costs. Competing on efficiency against optimized, stable, and existing civilian energy infrastructure will be relatively challenging. On the contrary, current methods for delivering energy effectively to remote, contested military environments are vulnerable and ripe for disruption. For these reasons, the US military will lead the way in developing new wireless power transfer technologies to merge logistics and tactics in a resilient, adaptive framework.

Ongoing Challenges

Human safety must be a core consideration of wireless energy web applications. For field-based effects, frequency selection mitigates the energy's interaction with biological materials. Further research is necessary to understand long-term effects and ensure that these systems do not interfere with other existing electrical devices, such as pacemakers.[36]

For beaming power, the dense core of these beams is likely to be harmful to anything in its path. Assured safety systems are possible by constantly monitoring the transmission path with a wider low-power beam and interrupting the high-power beam in response to intruders. Navy Research Labs demonstrated this safety protocol as part of their Power Transmitted Over Laser research effort, and this is a foundational goal for the DARPA POWER program.[37]

Ultimately these power-beaming systems will need to be designed with safety built in at the system level so that the system can be certified for operation versus for simply meeting current cumbersome requirements to coordinate laser shots individually with the Joint Service Laser Clearinghouse. While ensuring such system

34. Criswell, 17.

35. Kavadiki Veerabhadrappa et al., "Power Generation Using Ocean Waves: A Review," *Global Transitions Proceedings* 3, no. 2 (November 2022), https://doi.org/.

36. Isaac Chang et al., *RF/Microwave Interaction with Biological Tissues* (Hoboken, NJ: John Wiley & Sons, 2006).

37. Emanuel Cavallaro, "Researchers Transmit Energy with Laser in 'Historic' Power-Beaming Demonstration," US Navy, October 22, 2019, https://www.navy.mil/; and "Wireless Energy Relay."

safety remains a challenge, a successful analogy can be found in considering safe coexistence with the high-voltage power lines that are ubiquitous in the environment.

Although robust communication poses a challenge for wireless energy beaming networks, the existence of the network provides additional opportunities. Safe and effective power beaming requires an underlying low-power communication network to establish network protocols and control the flow of energy. As a result, a WEB network can be vulnerable to the same disruptions associated with traditional communications networks. Yet, because a WEB network provides a framework for many small, indefinitely persistent nodes, the overall reliability of both the networks is improved. Ultimately, the wireless energy web will reliably provide both energy and data using the communication links that are inherently necessary for effective power beaming.

As discussed earlier in this article, the rate or flux of energy transfer possible through wireless means is a challenge. Air refueling provides an extreme example of energy transfer rates possible with liquid fuels. Considering the full energy content of that fuel, the transfer rate during air refueling is equivalent to 2.5 gigawatts, which is orders of magnitudes greater than any laser conceived. Even with aggressive improvements in conversion efficiencies it would be impractical for most applications due to waste heat.

Though technologies will improve over time, there will be practical limitations to wireless power beaming transfer rates, which will limit applications. Yet early DARPA studies showed many meaningful military applications were feasible in the next few years with tremendous growth potential over the next decade.[38] Ultimately, though, improved distribution will not solve all energy challenges, and continuing the generation, storage, and distribution optimization methodology inherent to EWD will be necessary.

Conclusion

The energy web dominance framework provides a novel perspective on the fundamental character of warfare, revealing new metrics for optimizing military effects delivery. The current trend of buying fewer expensive, monolithic platforms that rely on liquid hydrocarbon fuels is unsustainable and vulnerable. Countering the peer adversary combat environment requires a new approach. Leveraging the electromagnetic spectrum to transmit energy wirelessly could enable a complementary network of persistent yet inexpensive platforms that are able to flexibly and resiliently focus military effects at a distance. Emerging technologies reveal a pathway to achieving this new vision.

The linkages in the wireless energy web will be built using a combination of magnetic resonance, optical, and radio frequency beams enabled by a host of supporting developments. To foster such a disruptive change, research should continue to probe the necessary families of technologies to find niche markets where wireless power transfer provides an immediate advantage. From there, the proven technologies can

38. Calhoun, "DARPA Energy Web Dominance."

be scaled into a larger network to achieve sweeping effects. This disruptive transformation will take investment in development, tactics, training, and procedures. Yet by achieving energy web dominance, the United States can maintain an advantage in great power competition for decades to come.[39] Æ

39. See Calhoun.

CYBER RED LINES

Government Responses to Cyberattacks on Critical Infrastructure

Denise L. Tennant
Louis Nolan
Deanna House

While the concept of red lines is relatively well-documented and discussed in areas of research surrounding deterrence and acts of war, the term *cyber red lines* is rather complicated and fairly immature in the research. Recognizing the ongoing challenges surrounding the red line term in a cyber context, this article seeks to define such a threshold within gray-zone cyber operations to determine an appropriate situation when the US Department of Defense could and should respond to state or nonstate actor operations that manifest as a cyberattack. The article also seeks to clarify what is meant by the term *cyber gray zone*.

Research surrounding red lines in terms of great power conflict and war provides an important area of study in order to understand what defines a red line and how it can be influential to conflict.[1] Red lines within a cyber context, however, are not as clearly articulated and represent an evolving concept with many complicated nuances. The amorphous nature of the cyberspace domain—unlike the air, land, sea, and even space domains—and the vaguely understood boundaries between US and adversary cyber terrain can prove problematic when drawing cyber red lines.

Furthermore, the ubiquitous nature of technology, and more specifically cyber-related technology, can create challenges in understanding and determining the role of the Department of Defense in response to offensive cyberspace operations (CO) by state and nonstate actors. Joint doctrine defines cyberspace operations as "the employment

Denise Tennant is deputy chief of operations of the Information Effect Directorate, Joint Warfare Analysis Center, in Dahlgren, Virginia, and holds a juris doctor from the Marshall-Wythe School of Law at the College of William and Mary.

Louis Nolan is a Department of the Air Force civilian at United States Strategic Command, Offutt Air Force Base, Nebraska, and holds a master of science in systems management from the University of Southern California.

Dr. Deanna House is an assistant professor of information systems and quantitative analysis, co-director of the Nebraska Deterrence Lab at the College of Information Science and Technology, and Cyber Threat Analysis Lab research lead, National Counterterrorism Innovation, Technology and Education Center, University of Nebraska Omaha.

1. See, for example, Thomas G. Mahnken and Gillian Evans, "Ambiguity, Risk, and Limited Great Power Conflict," *Strategic Studies Quarterly* 13, no. 4 (2019), https://www.airuniversity.af.edu/; and Derek Grossman and Joel Speed Meyers, "Minding the Gaps: US Military Strategy toward China," *Strategic Studies Quarterly* 13, no. 4 (2019).

of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" and includes not only military and intelligence but also DoD business components. Importantly, cyberspace operations can be malicious but are not always so.[2]

In the era of technological advancements, identifying strategic inflection points—points at which businesses or organizations undertake significant changes in order to remain competitive—is critical.[3] In the case of cyber strategic inflection points for the military, this means a move to develop capabilities superior to that of an adversary. Efforts to identify current cyber strategic inflection points and motivations that drive change create ongoing challenges surrounding when the Defense Department could and should respond to state or nonstate actor operations that manifest as a cyberattack.

Response to a cyberattack that results in an escalation beyond the virtual realm would typically not occur due to the nonphysical nature of attacks and their temporary and reversible effects.[4] The relationship between deterrence and red lines can be complicated in cyber-specific engagements, mainly due to attribution and to challenges surrounding capabilities.

In instances of cyberattacks, it can be difficult to know whether an attack will be effective due to the ever-changing network and software environment. Attribution can be hard to attain when responding to a cyberattack. Raising false flags and taking time to examine an attack forensically to determine its origin can prevent a swift response.[5] In addition, traditional deterrence methods that involve disclosing specific details about capabilities can provide adversaries with information that could result in preventing or deflecting an attack.[6] This article thus explores the concept of cyber red lines and provides a starting point for understanding what this means in terms of responses to cyberspace operations conducted by adversary state and nonstate actors.

In order to establish a baseline understanding of cyber red lines, this article relies heavily on legal and academic literature analyzing the current state of international law and norms applicable to cyberspace, official US policy documents on cyberspace and cyberspace operations, and proposed cybersecurity approaches, as well as on news reports and academic analyses of these operations.

---

2. *Joint Cyberspace Operations*, Joint Publication (JP) 3-12 (Washington, DC: Chairman of the Joint Chiefs of Staff, December 19, 2022), I-1.

3. Robert A. Burgelman and Andrew S. Grove, "Strategic Dissonance," *California Management Review* 38, no. 2 (1996), https://doi.org/.

4. Erica Borghard and Shawn W. Lonergan, "Public-Private Partnerships in an Era of Great-Power Competition," in "Ten Years In: Implementing Strategic Approaches to Cyberspace," *Newport Papers* 45 (2020), https://digital-commons.usnwc.edu/.

5. Joseph F. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016), https://doi.org/.

6. Davi M. D'Agostino et al., *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets*, GAO-10-147 (Washington, DC: Government Accountability Office, 2009), https://www.gao.gov/.

Defining Cyber Red Lines

This article defines a red line as the threshold at which an action taken is so grievous that a use of force in response would be generally accepted under international law. This definition sets the upper boundary for the gray zone, the nebulous area of actions that fall below the threshold of armed conflict but may still warrant a US government response. In this zone, cyberspace operations provide a unique context under which adversaries can hide activities, create uncertainty, and avoid attribution—all key components that blur the evidence that would warrant a use of force as a response.[7] Further defining the gray zone as it relates to CO and the thresholds for the DoD response to actions within it is part of the larger analytic focus of this article.

The term *red line* is frequently used, but in the case of cyber, it remains inadequately defined. The context-specific nature of cyberattacks creates an air of ambiguity surrounding consequences should a red line be crossed. There is rarely agreement on the term, with definitions ranging from "an expression used by governments to privately define a threshold for action" to "an unequivocal threat, a line in the sand that if crossed, the target would incur the full fury of the state that issued the threat in the first place."[8] This lack of common understanding creates an uncertainty that makes effective deterrence even more difficult.

The construct of red lines is prevalent in every continent with the number of red lines currently drawn at an all-time high.[9] Formal declarations of cyber red lines have made a recent appearance but remain vaguely developed and bring up the challenges in maintaining a state's moral credibility when responding to out-of-bounds attacks.[10]

The UN norms of responsible state behavior are intended to determine norms for appropriate cyber behavior in the interest of maintaining peace and security. Significant undertakings such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*—the 2013 academic manual that explored international law principles as they relate to cyber warfare and its 2017 follow up, respectively—also provide mechanisms for determining a starting point for behavior in the cyberspace domain.

7. Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020).

8. Bruno Tertrais, *The Diplomacy of "Red Lines": Recherches & Documents* (Paris: Fondation pour la Recherche Stratégique, February 1, 2016), https://www.frstrategie.org/; and Albert Wolf, "Backing Down: Why Red Lines Matter in Geopolitics," Modern War Institute, August 18, 2016, https://mwi.westpoint.edu/.

9. David Andelman, *A Red Line in the Sand: Diplomacy, Strategy, and the History of Wars That Might Still Happen* (New York: Pegasus Books, 2021).

10. Stephanie Pendino, Robert K. Jahn Sr., and Kirk Pedersen, "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light," *Campaigning: the Journal of the Joint Forces Staff College*, September 7, 2022, https://jfsc.ndu.edu/.

Yet existing norms are either lacking or still subject to debate, especially in strategic interstate competition short of armed conflict.[11]

Literature surrounding national security is replete with concerns about the establishment of red lines in general and cyber red lines in particular. One analysis of historical and current red lines, such as those drawn by China in the South China Sea that are "physical, diplomatic, military, [and] all too often existential," contends that such "lines in the sand" have "proliferated in recent years across every continent and . . . have reached a toxic apex in numbers and virulence at this very moment in history."[12] In pointing to their limitations, the analysis further notes that red lines work best only if both sides accept their parameters.[13] Moreover, an adversary can ignore a red line and force the United States to implement a response or action it does not desire to take. In a different vein, red lines can serve as a provocation, eliciting further activity as a psychological response to being told what not to do.[14]

In terms of establishing a cyber red line, an oft-cited concern is an adversary conducting gray-zone cyber actions that fall just below that line.[15] Additionally, as discussed above, it is not always possible to establish attribution with confidence and to act in a timely manner. Establishing norms for behavior that take the spectrum of cyberspace operations into consideration can be a useful starting point. The high-cost effects such as those targeting the general population that are physically destructive and potentially lethal and irreversible should be avoided on the offensive but also the defensive side.[16]

Yet establishing cyber red lines can have an advantage; the cyber red line argument is not one-sided. Lacking codified cyberspace international law or norms, red lines can address a void or gap within international law.[17] Despite some of the potential shortcomings noted above, the red line construct remains prevalent and can be useful to conceptually frame offensive cyberspace operations below the level of armed con-

11. Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013); Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge, UK: Cambridge University Press, 2017); Gary Corn, "Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, ed. Winston S. Williams and Christopher M. Ford (2018, forthcoming), https://papers.ssrn.com/; and Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (2017), https://doi.org/.

12. Andelman, *Red Line*, 1.

13. Andelman, *Red Line*.

14. Dan Altman and Kathleen E. Powers. "When Redlines Fail: The Promise and Peril of Public Threats," *Foreign Affairs*, February 2, 2022. https://www.foreignaffairs.com/.

15. Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022), 1, https://doi.org/.

16. Pendino, Jahn, and Pedersen, "Cyber Deterrence."

17. Andelman, *Red Line*.

flict.[18] Furthermore, red lines impact global perceptions of power and influence; research suggests the reputation of the United States may suffer if an adversary appears to cross a red line without generating an appropriate or implied response.[19]

Cyberspace Operations and the Cyber Domain

Securing information systems and technology to maintain continued operations of critical infrastructure (CI) is complicated due to the varying responsibilities of government and private sector entities. This is an ongoing and rapidly changing environment, with government-driven policies and compliance requirements offering guidance on how entities respond to attacks. Cybersecurity is vital to Americans' everyday lives, US society, and continued innovation. It is a must-succeed mission that supports the United States' survival as a sovereign nation. The United States must employ prudent measures to prevent adversaries from conducting cyberspace operations that cripple its ability to operate in the modern world and be prepared to respond appropriately if cybersecurity measures fail.

Attackers frequently target critical infrastructure, which can extend effects beyond that of a defense entity and could bridge the gap between the virtual and physical realms. Critical infrastructure, which includes both DoD and non-DoD assets and facilities, consists of "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters."[20] Examples of CI sectors include energy, dams, communications, and the defense industrial base. Reliance by the Department of Defense on CI could affect core missions and assets.

Cyberspace, a global domain within the information environment, complements the four physical DoD warfighting domains yet is distinct as both the public and private sectors operate ubiquitously in cyberspace and rely on civilian networks and infrastructures to conduct basic functions.[21] Some 90 percent of US critical infrastructure is operated by the private sector. The expanding reliance on small business technology firms, academic institutions, and federally funded research and development centers to conduct state-of-the-art research as part of the defense ecosystem

18. Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), https://doi.org/.

19. Altman and Powers, "When Redlines Fail."

20. Joseph R. Biden Jr., National Security Memorandum on Critical Infrastructure Security and Resilience, NSM-22, April 30, 2024, https://www.whitehouse.gov/.

21. JP 3-12.

frames the dependency on the private sector to advance and secure US society and its economic engine.[22]

Cyberspace operations against US critical infrastructure and other private sector businesses pose new challenges, but these cyberattacks and the appropriate responses to them must be considered within the framework of existing international law. The ability of states to respond to adversary CO in times of conflict is addressed by experts in international law, but uncertainty remains concerning when and how it is appropriate for the Department of Defense to respond in peacetime, particularly if the target is not military in nature.[23] The *Tallinn Manual 2.0* outlines the current understanding of international law surrounding state CO in peacetime but also identifies numerous areas where experts are not in agreement about what international law requires.[24]

As early as 1984, the opportunity to exploit data "from converging telecommunications and automated information systems" was seen as a risk to US security.[25] In 1995, cyber threats to the energy sector, one of the 16 CI sectors, foreshadowed an evolving, nonkinetic means to threaten the US homeland.[26] Applying the Cold War construct of nuclear deterrence, the US response to adversary CO, to include that against US critical infrastructure and private sector businesses, was couched in a "cyber deterrence" framework.[27] Yet scholars and practitioners found the approach to be too responsive, not proactive, and not effective as "adversary CO and campaigns targeting US interests over that period . . . increased in frequency, scope, scale, and sophistication."[28]

The Cyberspace Solarium Commission, the bipartisan intergovernmental organization established under the 2019 National Defense Authorization Act to determine a strategy for US cyberspace defense, devised the layered cyber deterrence approach to curtail the "probability and impact of cyberattacks of significant consequence" via the three complementary ways of shaping behavior, denying benefits, and imposing

22. Micah Zenko, "Reading between the Red Lines: Deterrence and US Foreign Policy," Lessons for History Series, Council on Foreign Relations, May 10, 2021, audio podcast and YouTube video, 04:51, https://www.cfr.org/; and Lloyd J. Austin III, *National Defense Strategy of the United States of America including the 2022 Nuclear Posture Review and the 2022 Missile Posture Review* (Washington, DC: Department of Defense, October 27, 2022), https://media.defense.gov/ .

23. Schmitt, *Tallinn Manual*.

24. Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 735, https://www.law.georgetown.edu/; and Schmitt, *Tallinn Manual 2.0*.

25. Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

26. Michael Warner, "A Brief History of Cyber Conflict," in "Ten Years In"; Barack Obama, Critical Infrastructure Security and Resilience, Presidential Policy Directive – 21 [PPD-21], February 12, 2013, https://obamawhitehouse.archives.gov/; and Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, "Preface," in "Ten Years In."

27. Libicki, *Crisis and Escalation*.

28. Schneider, Goldman, and Warner, "Preface," 45; and Michael P. Fischerkeller and Richard J. Harknett, *Initiative Persistence as the Central Approach for US Cyber Strategy*, IDA Document NS D-22719 (Alexandria, VA: Institute for Defense Analysis, 2021), https://www.ida.org/.

costs.[29] The move away from the traditional "response force"–focused concept—responding after an attack—and into offensive cyber capabilities is necessary to maintain effective cyber deterrence strategies.

This shift from response-force/defensive actions to an offensive approach necessitates understanding the term *persistent engagement*, which is defined as "a use of cyber capabilities in continuous contact with adversaries to generate tactical, operational, and strategic initiative (and thus set the conditions of security in our favor in a constantly changing domain)."[30]

In a similar manner, persistent engagement has also been referred to in the literature as initiative persistence, which has been proffered as the central focus for US national cyber strategy and is defined as "a strategic approach to preclude, mitigate, and counter strategically consequential cyber action occurring continuously short of armed conflict." It stresses the need to compete continuously—the crux of US Cyber Command's persistent engagement doctrine—in the gray zone of CO and not cede the domain to the adversary.[31] These concepts have emerged to fill the perceived void in US deterrence theory as applied to actions within the cyber gray zone.[32] In short, cyber conflict is ongoing and constant.

In terms of the current cyberspace terrain, the notion of a second strategic inflection point within the cyber domain is trending.[33] The first strategic inflection point occurred in 2013 when adversaries commenced "operat[ing] continuously against CI, government networks, defense industries, and academia—both in America and abroad."[34] After this point, there was a significant expansion when the cyber threat shifted from espionage and exploitation to disruption and data deletion.[35]

In 2020 the Cyberspace Solarium Commission's report highlighted a second strategic inflection point focused on adversaries' targeting of cyber and related technologies that "improve the quality of human life." Further, it noted that "threats continue to grow at an accelerating pace" and that "America is facing adversary nation-states, extremists, and criminals that are leveraging emerging technologies to an unprecedented degree."[36] This is driving the need for public-private partnerships when fighting adversaries.

Individual responses by private sector entities, however, are complicated by the Computer Fraud and Abuse Act—also referred to as the antihacking law—which prohibits any unauthorized access to a computer, either knowingly or unintentionally.[37] Conducting defensive activities that violate the act is considered illegal and

29. Angus King et al., *Report of the United States of America Cyberspace Solarium Commission* (Washington, DC: Cyberspace Solarium Commission, March 2020), https://cybersolarium.org/.
30. Schneider, Goldman, and Warner, "Preface," 45.
31. Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, 1.
32. Paul M. Nakasone, "A Cyber Force for Persistent Operations," in "Ten Years In."
33. Nakasone, "Persistent Operations," 45; and King et al., *Cyberspace Solarium*.
34. Nakasone, 45.
35. Schneider, Goldman, and Warner, "Preface," 45.
36. King et al., *Cyberspace Solarium*.
37. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986).

is a punishable offense. Thus, the private sector looks to government entities to assist with responding to activities that edge into areas of national security and defense. The recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 has further constrained the responsibilities of private sector entities to reporting only and places the onus of a response on the government.[38] In addition, adversary actions in the cyber domain are an increasing concern as a part of hybrid warfare, which includes conventional and unconventional tactics conducted by a spectrum of state and nonstate actors and blurred together in an uncharacterized fashion.[39]

While cyberspace is still a maturing domain, numerous case studies exist that explore the actors; the specific tactics, techniques, and procedures employed by the cyber attacker and during the subsequent response by the target; the impact to the target; and the ramifications for cyber norms.[40] One example focuses on Russia's alleged cyberattack on US government and private sector networks via the US information technology company SolarWinds.[41] Ransomware attacks on municipalities, health care facilities, and school systems and breaches of consumer data and potential release of personally identifiable information are routinely in the news. Recent attacks have trended toward critical infrastructure and have brought to light vulnerabilities that exist in the aging infrastructure of the United States.[42] Who and what organizations are best postured to respond to these cyberattacks is frequently debated. Which organization, acting within statutory constraints and in alignment with international law and norms, should be granted affirmative authority to conduct offensive cyberspace operations is also under debate.[43]

International Law and Cyberspace Operations

With so much uncertainty regarding what state conduct is permissible in the cyber domain, this article intentionally sets a high bar for crossing the cyber red line. Making a connection between the virtual and physical world is best understood in terms of effects and by taking into consideration what in the cyber world constitutes an attack that is equivalent

38. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity and Infrastructure Security Agency (CISA), accessed June 5, 2024, https://www.cisa.gov/.

39. Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), https://potomacinstitute.org/.

40. Faisal Quader and Vandana P. Janeja, "Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies," *Journal of Cybersecurity and Privacy* 1, no. 4 (2021), https://doi.org/; and Marcus Willett, "Lessons of the SolarWinds Hack," *Survival: Global Politics and Strategy* 63, no. 2 (2021), https://doi.org/.

41. Willett.

42. Raphael Satter, "US Warns Hackers Are Carrying Out Attacks on Water Systems," Reuters, March 20, 2024, https://www.reuters.com/; and Sophia Fox-Sowell, "'We Know They're on the Network,' CISA Official Says of Nation-State Actors Infiltrating U.S. Critical Infrastructure," StateScoop, March 19, 2024, https://statescoop.com/.

43. Corn, "Cyber National Security."

to a conventional attack.[44] The definition of a red line stated previously assumes there is a threshold accepted by the international community at which an armed attack using CO would warrant a permissible response of self-defense by the targeted state.

This section examines international law and norms as they apply to the use of force in general, and how they are understood to apply to actions in the cyber domain in particular. Cyberspace operations conducted by states that do not cross the cyber red line but are not recognized as permitted state activity under international law fall into the cyber gray zone. In recent years, the cyber gray zone has extended into commercial entities and civilian populations, further complicating and broadening the scope of permitted state activity.[45]

The United States has long recognized the applicability of existing international law to the cyber domain, acknowledging the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. [Instead,] long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[46] The primary body of international law regulating when states may use force—jus ad bellum—is rooted in the principles of sovereignty and nonintervention. Sovereignty includes the right of a state to control access to its territory and to exercise jurisdiction and authority on its territory.[47] The principle of nonintervention gives each state the right to conduct its own affairs without outside interference.[48] The two types of state practices that run afoul of the principles of sovereignty and nonintervention are the use or threat of "force" and the use of nonforceful but coercive intervention.[49]

The prohibition against the use or threat of force is found in article 2(4) of the UN Charter: "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[50] The UN Charter does not offer a definition of the use of force, nor has an authoritative definition been accepted by the in-

44. Ron Granieri and Patrick Walsh, "If-Then: Defining the Red Line in Cyberspace," April 19, 2022, in *A Better Peace: A War Room Podcast*, podcast, MP3 audio, 31:45, https://warroom.armywarcollege.edu/; and Catherine A. Theohary, "Use of Force in Cyberspace," In Focus (Washington, DC: Congressional Research Service, June 25, 2024), https://crsreports.congress.gov/.

45. Cassandra Steer, "International Humanitarian Law in the 'Grey Zone' of Space and Cyber," CIGI Essay Series: Cybersecurity and Outer Space, CIGI [Centre for International Governance Innovation], January 29, 2023, https://www.cigionline.org/.

46. Obama, PPD-21.

47. Schmitt, *Tallinn Manual.*

48. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), Judgment, 1986 I.C.J. Rep. 14 (June 27), https://www.refworld.org/.

49. Peter Z. Stockburger, "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum," *American University International Law Review* 31, no. 4 (2016), https://digitalcommons.wcl.american.edu/.

50. United Nations [UN] Charter, 1945, article 2(4), https://www.un.org/.

ternational community. The International Court of Justice has stated the prohibition on use of force applies to "any use of force, regardless of the weapons employed."[51]

The United States has long taken the position that the "inherent right of self-defense potentially applies against any illegal use of force . . . [and] there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[52]

The principle of nonintervention has recognized exceptions, but generally, intervening in a state's choice of a "political, economic, social and cultural system, and the formulation of foreign policy" is not permitted.[53] Yet, this is not a complete bar to state action, as states may still promote and encourage the fulfillment of self-determination rights within another state.[54]

International efforts to answer outstanding questions of how existing laws and norms apply to cyberspace resulted in the *Tallinn Manual* and are supplemented by the *Tallinn Manual 2.0*.[55] The rules set forth in these two manuals are an attempt by the so-named International Group of Experts to capture the current state of international law and norms but are nonbinding on states and may continue to evolve with changing national interests in cyberspace.

Scholarship has identified three main approaches for determining if a cyberspace operation crosses the threshold to be considered a use of force or armed attack under international law: an instrument-based approach, which looks at the form of weapon used and whether the attack possesses the physical characteristics traditionally associated with military coercion; the target-based approach, which treats any CO against critical infrastructure as an armed attack; and the effects-based approach, which focuses on the overall effects of the CO and considers factors such as severity, immediacy, and directness of harm.[56]

Taking the three approaches into consideration, cyberspace operations "constitute 'armed attack[s]' when they are aimed at causing irreversible disruption or physical damage to a cyber-physical system, which is a physical system monitored or controlled by computers."[57] The term *significant* is also an important consideration when identifying if damage from a cyberattack warrants a use of force.[58] But if the intended disruption or damage is trivial, or the cyberattack is aimed at causing disruption or damage to computers or networks that do not monitor or control physical systems,

51. "Legality of the Threat or Use of Nuclear Weapons. Overview of the Case," International Court of Justice, accessed June 5, 2024, https://www.icj-cij.org/.

52. Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (2012): 7, https://journals.law.harvard.edu/.

53. Nicar. v. US.

54. Stockburger, "Known Unknowns," 31.

55. Schmitt, *Tallinn Manual*; and *Tallinn 2.0*.

56. Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," *Joint Force Quarterly*, no. 67 (2012), https://ndupress.ndu.edu/; and Reese Nguyen, "Navigating Jus Ad Bellum in the Age of Cyber Warfare," *California Law Review* 101, no. 4 (2013): 1083–4, https://lawcat.berkeley.edu/.

57. Nguyen, 1084.

58. Akber Khan, "Deterrence and the Problem of Attribution in Cyberspace: An Analysis of Vulnerabilities and Options for Pakistan," *Balochistan Think Tank Network Journal* 1, no. 2 (2022): 6–7.

"the action could be considered an illegal 'use of force' or an 'armed attack' justifying responsive force, depending on the gravity of the intended or reasonably foreseeable consequences."[59] This approach has considerable merit, but as discussed below, it is incomplete without the consideration of several additional factors.

As mentioned, a recurring issue in the cyber domain is that of attribution—assigning responsibility for a CO to a state or nonstate actor. In the Nicaragua v. United States case, the International Court of Justice found that a state with "effective control" over nonstate actors is responsible for those acts, at least within the context of military operations.[60] The International Criminal Tribunal for the Former Yugoslavia adopted a different threshold of "overall control," requiring state participation in the planning and supervision of military operations.[61] In general, international law will find the conduct of a person or group of persons to be "considered an act of a state under international law if the person or group of persons were acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[62]

A discussion of international laws relating to cyberspace operations would be incomplete without mentioning the one specific type of operations that is not viewed as a violation of international laws and norms, namely espionage. Espionage, whether through traditional physical methods or through CO, is generally tolerated by the international community during peacetime, "because, among other things," it "can reduce the chance of a misunderstanding that could lead to a real conflict."[63] But recent attacks targeting critical infrastructure and those that seek to interfere with elections are becoming destructive enough to be considered cyber warfare and thus moving toward a cyber red line.[64]

The state that is the target of an espionage operation might rightly choose to respond with punitive measures, but ordinary cyberspace operations to conduct espionage are not included in this analysis. In the example of the SolarWinds attack, which had underlying goals of espionage, the appropriate response would be for the United States to make it difficult for Russia to conduct espionage but not expect it to be prevented entirely.[65]

Establishing Cyber Red Line Norms

Preventing and responding to the unique challenges of adversary actions in the cyber domain require a whole-of-nation investment. One part of the US strategy is integrated deterrence, which uses every tool at the Department of Defense's disposal

59. Nguyen, "Jus Ad Bellum," 1084.

60. Nicar. v. US.

61. Stockburger, "Known Unknowns," 31.

62. International Law Commission, "Responsibility of States for Internationally Wrongful Acts," in *International Documents on Environmental Liability*, ed. Hannes Descamps, Robin Slabbinck, and Hubert Bocken (Dordrecht, Netherlands: Springer Science + Business Media, 2008), https://link.springer.com/.

63. Willett, "SolarWinds Hack," 12.

64. Kevin Townsend, "NATO Draws a Cyber Red Line in Tensions with Russia," SecurityWeek, May 13, 2024, https://www.securityweek.com/.

65. Willett, "SolarWinds Hack," 20.

in close coordination across the US government and with Allies and partners to deter aggression by other states.[66] This involves integrating across military domains—land, air, maritime, space, and cyber—and nonmilitary domains, including economic, technological, and information.[67]

While the Department's role in defending against or responding to gray-zone cyberattacks against US critical infrastructure and other private sector businesses is becoming clearer, its appropriate response remains less clear. Within its eight Unified Command Plan mission areas, strategic deterrence is the logical avenue for addressing gray-zone cyberattacks, drawing upon integrated deterrence as a mechanism to combine capabilities across regions, domains, the spectrum of conflict, the US government and Allies and partners.[68]

Strategic deterrence entails far more than nuclear operations and nuclear deterrence. Particularly in situations where tensions are already heightened, cyberspace operations could contribute to a strategic deterrence failure. The role of strategic deterrence is to make the cost to adversaries high enough that they do not take military action against the United States, its national interests, and its Allies and partners. Considerations for understanding the intensity of gray-zone attacks can bridge the cyber-specific gap between strategic and integrated deterrence.

Conclusion

While a gray-zone cyberattack against US critical infrastructure or private sector businesses might not look like a traditional kinetic attack, the outcomes and harms from a cascading cyberattack could rapidly exceed the damage from one or even several conventional kinetic weapons. The importance of effects—such as irreversible damage—and attribution are key elements in understanding cyber red lines. This article provides a starting point for future academic research to examine the details of specific cyber operations to determine if these operations threatened the target state's "sovereignty, peace, and security."[69]

The International Group of Experts that created the *Tallinn Manual* and *Tallinn Manual 2.0* could not agree on what would constitute a cyber "armed attack," with some adopting an approach that limited it to physical effects and others supporting an approach that focused on the severity of the effects and did not require they be physical in nature.[70] Norms around the use of CO are still developing, leading to ambiguity in terms of what constitutes an attack that would warrant the use of force, much less the threat of force, in response as defined in international law.

---

66. Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: White House, October 2022), https://www.whitehouse.gov/; and King et al., *Cyberspace Solarium*.

67. Biden.

68. Biden; 2022 Unified Command Plan, Memorandum of the Secretary of Defense, 88 Fed. Reg. 26219 (January 13, 2021); and Austin, *National Defense Strategy*.

69. Nguyen, "Jus Ad Bellum," 1125.

70. Stockburger, "Known Unknowns," 31.

Defense and homeland security entities must coordinate efforts in order to understand the gravity of potential attacks and to respond appropriately. Providing mechanisms for timely analysis of an attack to clearly determine attribution is also needed. Additional research and clarification are necessary to work toward agreed-upon terms for cyberspace operations and gray-zone activities. Defining appropriate actions related to a response once attribution is determined will also clarify the course of action the government under attack should take. In addition to potential physical damage, defense entities should not underestimate the potential negative impact of significant gray-zone cyberattacks from digital, economic, and societal harm perspectives as the Department strives to deter those actions that threaten national security. Æ

EFFECTIVE ASSURANCE

A Strategic Imperative

LUKE R. STOVER

Assurance of Allies and partners, particularly in the strategic realm of nuclear weapons, is often viewed as ancillary to the larger objective of deterrence. Yet assurance, which seeks to influence the decision of Allies and partners, is fundamentally different than deterrence, even extended deterrence, which aims to shape the decisions of potential adversaries. A proper understanding of assurance is critical in an age of renewed great power competition, where alliances and partnerships provide an asymmetric strategic advantage over potential adversaries. This article proposes a robust definition of assurance as the perpetual process and product of actions taken to enhance an ally's or partner's confidence in the securities provided through United States' military capability and national will. Such assurance must not only be sustained and continually recalibrated but also primarily viewed from the perspective of the assured, to ensure a democratic world order and continued nonproliferation of nuclear weapons.

A commonly stated goal of many US military activities, especially in the strategic realm of nuclear weapons, is to deter potential adversaries and assure Allies and partners.[1] Yet the goal of assurance can become subsumed in such discussions, either conflated with or subordinated to a larger deterrence objective. Even informal discussions among practitioners are often quick to address the deterrent value of a safe, secure, and effective nuclear capability, while the significance of assurance to US Allies and partners provided by that same capability becomes almost an afterthought.

Yet in an era of renewed great power competition, alliances and partnerships—which have always been important—are more critical than ever. These relationships provide an asymmetric strategic advantage; strong alliances and partnerships are built and sustained through strong assurances.[2] Therefore, understanding and prioritizing

Colonel Luke Stover, USAF, is deputy commander of the 377th Test and Evaluation Group at Vandenberg Space Force Base, California.

1. This article is based on a paper written under the auspices of the Los Alamos National Lab.

2. Lloyd J. Austin III, *2022 National Defense Strategy of the United States of America including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, October 2022), https://media.defense.gov/.

assurance bolsters the strategic position of the United States and its Allies and partners. Relegating assurance to an appendage of deterrence or assuming it is a foregone conclusion will detract from America's strategic advantage. Both Secretary of State Antony Blinken and Secretary of Defense Lloyd J. Austin have articulated this very issue:

> Our alliances are what our military calls "force multipliers." We're able to achieve far more with them than we could without them. No country on Earth has a network of alliances and partnerships like ours. It would be a huge strategic error to neglect these relationships. And it's a wise use of our time and resources to adapt and renew them, to ensure they're as strong and effective as they can be.[3]

Despite such directives from defense leaders, the current understanding, implementation, and practice of assurance remains ill-defined. Assurance should be studied, developed, and nurtured as a strategic imperative to ensure the force multiplier provided by strong alliances and partnerships. This article sees assurance as the process and product of actions taken to enhance an Ally's or partner's confidence in the United States' military capability and national will. Such an understanding recognizes assurance as a perpetual and iterative progression, where constant vigilance is required to sustain and calibrate relationships between the United States and its Allies and partners.

Furthermore, effective assurance, which must be primarily viewed from the perspective of the assured, is contingent upon credible capabilities, demonstrated past actions, perpetual integration of Allies and partners, and a compelling vision of the expected outcomes of assurance. Such outcomes include a trend toward a democratic world order and continued nonproliferation of nuclear weapons. The strategic implications of these outcomes are of principal importance in persistent great power competition.

Distinctions from Deterrence

In strategic discussions, deterrence and assurance are often used in the same breath, yet the two are fundamentally different. Understanding the one thus helps to understand the other. The idea of deterrence, both as a theory and a strategy, occupies the minds of numerous academics and military professionals as much today as it has for the past 80 years. For the purposes of this article, deterrence is defined as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[4] This definition can be further distilled as the equation

Deterrence = Capability x Will

3. Antony J. Blinken and Lloyd J. Austin III, "America's Partnerships Are 'Force Multipliers' in the World," *Washington Post*, March 14, 2021, https://www.washingtonpost.com/

4. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense (DoD), 2024), s.v. "deterrence," accessed May 31, 2024, https://jdeis.js.mil/.

which recognizes that "reliable deterrence is achieved only when potential adversaries perceive the multiplying effect of our capabilities and our will."[5] If either military capability or national consensus of will is absent, then deterrence as a product is null.

The simplicity of this equation obscures the fact that myriad distinctions stem from the core concept of deterrence.[6] These distinctions include but are not limited to deterrence by denial, deterrence by punishment, general deterrence, immediate deterrence, easy deterrence, difficult deterrence, direct deterrence , and extended deterrence.[7] While there is an abundance of literature on the topic of deterrence and its many iterations, a detailed review is beyond the scope of this paper. Without addressing each of these subsets in turn, this article briefly addresses the idea of extended deterrence, which is particularly germane to a discussion of assurance.

Assurance Defined

The concept of extended deterrence, wherein a US deterrent capability is projected to prevent a potential adversary's actions against an ally, is clearly intertwined with the concept of assurance; however, they are not synonymous. Deterrence, including extended deterrence, is aimed at shaping the decision calculus of potential adversaries. Assurance, on the other hand, is intended to shape the decisions of allies.

Just as there are different forms of deterrence, there are various forms of assurance. One study delineates four primary variants of assurance used throughout policy and strategy literature.[8] First, assurance may be viewed as a component of deterrence. This variant of assurance is the proverbial carrot to be used in harmony with a deterrent stick. If a state heeds a deterrent, it will reap benefits by means of assurances.

Second, reassurance is a means by which one state assures another that its intentions are not aggressive. Third, nonproliferation-related security assurances address policy issues regarding the spread of nuclear weapons. The fourth and final variant of assurance is what is termed alliance-related assurance. This variant of assurance is fostered between treaty allies as a commitment to mutual defense. This article is primarily focused on the fourth variant and includes considerations of partners, although the nonproliferation variant is also relevant to the discussion.

Assurance is not formally defined by the Defense Department. While the *DOD Dictionary of Military and Associated Terms* includes assure and deter as strategic effects, it does not define the terms *assure* or *assurance*. Perhaps the closest the Department

5. Russell Dougherty, "Capability x Will = Deterrence," *Air & Space Forces Magazine*, June 1, 1984, https://www.airandspaceforces.com/.

6. Michael J. Mazarr, *Understanding Deterrence* (Santa Monica, CA: RAND Corporation, April 19, 2018), https://www.rand.org/.

7. Keith B. Payne, "The Great Divide in US Deterrence Thought," *Strategic Studies Quarterly* 14, no. 2 (2020), https://www.airuniversity.af.edu/.

8. Jeffrey W. Knopf, "Varieties of Assurance," *Journal of Strategic Studies* 35, no. 3 (2012), https://doi.org/.

has come to defining the term was in the 2022 *Nuclear Posture Review*. Here, effective assurance of Allies and partners is characterized as

> built on a shared view of the security environment and deterrence challenges; a commitment to risk- and burden-sharing, modern and effective nuclear forces; robust consultation processes; and Ally and partner confidence that the United States has the will and capability to meets its security commitments.[9]

This is a maturation of earlier ideas of actively assuring Allies and partners, as expressed in the 2001 *Quadrennial Defense Review*. Here, the Department of Defense categorized assurance as the United States' commitment to "honor its obligations and . . . be a reliable security partner." It further notes, "Through its willingness to use force in its own defense and that of others and to advance common goals, the United States demonstrates its resolve and steadiness of purpose and the credibility of the US military to meet the Nation's commitments and responsibilities."[10] This excerpt captures the essence of assurance but falls short of a formal definition.

Outside the Defense Department, assurance is defined in equally limited and informal ways. The National Research Council, for example, posits that assurance is "convincing an ally of U.S. commitment to and capability for extended deterrence for the purpose of dissuading the ally from developing its own nuclear arsenal."[11] While this definition adequately captures key principles such as commitment and capability, it restricts the end goal of assurance to nonproliferation. Other vague definitions include "an attempt to increase an ally's feeling of security from external threat" and an objective that "requires the easing of allies' fear and sensitivities."[12] The paucity of formal definitions of assurance in military literature lends credence to the thesis that assurance is often an afterthought or appendage to deterrence. Given the importance of assurance, a formal definition will enhance mutual understanding of the concept and bridge connections between US policy and military strategy.

Therefore, this article proposes the following definition of assurance: *The process and product of actions taken to enhance an Ally's or partner's confidence in securities provided through the capability and will of the US government.* This definition reflects three key attributes of the concept. First, assurance is both a process and a product. It is never only an end result, but rather a perpetual and iterative progression. It is a

9. Lloyd J. Austin III, *2022 Nuclear Posture Review* (Washington, DC: Office of the Secretary of Defense, 2022), 14, https://media.defense .gov/.

10. *Quadrennial Defense Review* (Washington, DC: DoD, 2001), 11, https://dod.defense.gov/.

11. National Research Council of the National Academies, *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment* (Washington, DC: National Academies Press, 2014), 24, https://nap.nationalacademies.org/.

12. Brian Blankenship and Erik Lin-Greenberg, "Trivial Tripwires?: Military Capabilities and Alliance Reassurance," SSRN [Social Science Research Network], September 21, 2021, https://papers.ssrn.com/; and Keith B. Payne, "On Nuclear Deterrence and Assurance," *Strategic Studies Quarterly* 3, no. 1 (2009): 46, https://www.jstor.org/.

prime example of an "infinite game."[13] Second, the variables that make deterrence effective, capability and will, also make assurance effective. Third, the effectiveness of assurance must always be assessed from the perspective of the ally, not just from the perspective of the United States.

Alliances and Partnerships: The Root of Assurance

As previously stated, assurance shapes the decisions of Allies and partners. Therefore, a proper understanding of assurance is rooted in a clear understanding of alliances and partnerships—why states choose to form these relationships and why they remain. Security studies scholar Glenn Snyder's work is helpful here and can be extended in theory for the purposes of the article to apply to partnerships as well. He asserts that in a multipolar international system, where security is of primary importance, nations will form alliances for two reasons: "(1) some states may not be satisfied with only moderate security, and they can increase it substantially by allying if others abstain; [and] (2) some states, fearing that others will not abstain, will ally in order to avoid isolation or to preclude the partner from allying against them."[14] This is, in short, a game-theory-centered answer to the question of why states enter into these relationships.

Snyder also addresses the question of why states remain in alliances by examining a cost-benefit analysis between the primary risks of alliances: abandonment and entrapment.[15] Broadly, abandonment is the risk that an Ally will not hold up its end of a security agreement. Conversely, entrapment is the risk that a state will be compelled to fight a war, for which it holds little or no interest, in defense of an Ally. Alliances hold "both prospective good and prospective bad consequences; and the 'goods' and 'bads' for each alternative tend to be the obverse of those of the other."

In an alliance security dilemma, the "principal 'bads' " are abandonment and entrapment and "the principal 'goods' are a reduction in the risks of being abandoned or entrapped by the ally."[16] This logic also helps to explain the alliance gradient that exists from formal alliances to partnerships, to friendly nation relationships to positions of neutrality. The more formal an alliance, the higher the risks—and potential rewards—of the alliance relationship. To tilt any Ally's perception in favor of continued alliance, where the benefit outweighs the risk, the United States must actively cultivate and nurture a mindset of effective assurance. To understand the process and product of assurance is to understand the dynamics of US relationships with its partners and Allies, as the one depends on the other.

13. Simon Sinek, *The Infinite Game* (London: Portfolio Penguin, 2020).

14. Glenn H. Snyder, "The Security Dilemma in Alliance Politics," *World Politics* 36, no. 4 (1984): 462, https://doi.org/.

15. Snyder, 466.

16. Snyder.

Elements of Effective Assurance

Effective assurance can be measured by several factors. Snyder proposes five determinants that states consider as part of the alliance security dilemma: (1) relative dependence of the partners on the alliance, (2) strategic interest of Allies in defending each other, (3) explicitness of alliance agreements, (4) the degree to which an Ally's interests are in conflict with a potential adversary, and (5) recent past behavior of Allies.[17]

When viewed through the lens of assurance, these determinants may be expressed in a similar form. To effectively assure Allies and partners, the United States demonstrates its capability and will through (1) robust capabilities, (2) past actions, (3) a compelling vision, and (4) perpetual integration. Therefore, assurance may be expressed as

Assurance = Robust Capabilities x (Past Actions + Compelling Vision + Perpetual Integration)

The first variable, robust capabilities, addresses Snyder's first determinant, relative dependence. The United States must maintain robust capabilities that contribute to the collective security of an alliance. This variable is multiplicative and must be present for assurance to be effective. The next three variables are congruent with Snyder's final four determinants in that they collectively encompass the concept of will. These variables seem to be additive rather than multiplicative: assurance may exist—albeit in a limited capacity—with varying degrees of these variables, but each undoubtedly adds to or subtracts from it.

Robust Capabilities

A broad range of robust capabilities is paramount to US assurance of Allies and partners. The cornerstone of such capabilities is a safe, secure, and effective nuclear deterrent. Nuclear weapons are a foundational capability that serve as the backstop for deterrence and assurance alike. As long as nuclear weapons exist in a geostrategic context, the sustainment and modernization of the United States' nuclear stockpile and delivery systems must remain a fundamental, enduring priority in US national security strategy. Yet while the effective assurance of Allies and partners starts with a strong nuclear deterrent posture, it does not end there. Nuclear weapons cannot, and should not, be used to deter or assure in every situation.

Instead, nuclear weapons must be complemented by a broad range of military, information, diplomatic, and economic capabilities better suited to influence a potential adversary's actions across the competition continuum.[18] This is the idea behind

17. Snyder, 471–75.

18. *Joint Warfighting*, Joint Publication 1, vol. 1 (Washington, DC: Chairman of the Joint Chiefs of Staff, August 27, 2023), I-1, https://jdeis.js.mil/.

integrated deterrence, a hallmark of the 2022 *National Defense Strategy*.[19] Likewise, integrated assurance, wherein all instruments of national power are used in concert to positively assure Allies and partners, must also become part of the US defense lexicon. As such, the development and fielding of future US capabilities should include a deliberate assessment of what, if any, assurance they may be able to provide to allies and partners.

The intellectual and industrial capacity to develop, design, build, and field future capabilities is, in and of itself, a fundamental capability. This capability has been a core competency of the United States for the past 120 years. Yet, as the twenty-first century continues to shift from an era of warfare characterized by industrial capacity toward an era characterized by information-centric technologies, the United States must continue to shift its capabilities in kind.

Artificial intelligence, machine learning, microelectronics, and metadata are all ubiquitous terms in the modern age. The familiarity of these terms, however, should not undermine the critical implications of these information-centric technologies, and others like them, for the effectiveness of US assurance strategies in great power competition. As one scholar asserts, "Emerging technology is diffusing into an international system in which the United States has been the world's leading power for the past several decades."[20] Understanding the character of twenty-first-century warfare is paramount to developing the right capabilities for present and future conflicts.

Past Actions

Past actions inform the present and often shape the future. History is replete with examples of US actions that enhanced an Ally's confidence in the capability and will of the US government. Perhaps the clearest example is the stalwart commitment of the United States in World War II in the Pacific and European Theaters. Although the Japanese attack on Pearl Harbor and the subsequent declaration of war from Germany and Italy forced America's hand to enter the conflict, the scale and scope of the US response are categorically remarkable. The resolute demonstration of the US capability to energize a burgeoning industrial base to produce weaponry and war materiel on an unprecedented scale, coupled with the will to employ such capability, clearly shaped the outcome of the war.

The primary point of this example—while perhaps an oversimplification of US involvement in World War II—is that the demonstration of US capability and will brought an extraordinary level of assurance among Allies. The United States assumed the mantle of leadership in shaping the postwar international order upon this foundation of assurance, the most significant product of which was the establishment of NATO, an alliance of enduring political and military importance.

19. Jim Gamarone, "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says," DoD, December 8, 2021, https://www.defense.gov/.

20. Matthew Kroenig, "Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In," *Strategic Studies Quarterly* 15, no. 4 (2021), https://www.airuniversity.af.edu/.

Certainly, there are historical examples of the inverse, where US action, or inaction, detracted from an Ally's or partner's confidence in the capability and will of the US government. The point is one of perspective. Assurance does not start, or end, with the policies and actions of today. Assurance must be viewed through the long lens of history. In the same way that US actions during World War II shaped Allied perceptions for generations, so will US actions today shape such perceptions well into the future. That future age, shaped by a compelling vision, is also vitally important to assurance.

Compelling Vision

To what end? This is a fundamental question that shapes deterrence and assurance theory alike. Every strategic action should be framed by a future goal, objective, or end state. Without a clear and compelling vision of what lies ahead, it is exceedingly difficult to convince Allies and partners to journey alongside. Strategic objectives rarely perfectly align between states. Yet the more plainly the United States defines and articulates its grand strategy, seeks consensus from allies early and often, and tailors efforts by region, the greater the assurance provided.

Great power competition is, at its core, a tension between competing worldviews. The development and nourishment of a free, open, and democratic society has long been a strategic objective of the United States. The more clearly the United States can demonstrate and articulate the merits of democracy, the stronger its position by which to assure like-minded Allies and partners.

The Biden Administration's Summit for Democracy in December 2021 aimed to do just that. The free and open exchange of perspectives among democratically elected leaders from over 100 states certainly reinforced the merits of democracy to a global audience. But the summit also highlighted the need to protect and nurture the idea, or vision, of what democracy should be. As President Joseph R. Biden previously stated, "Democracy doesn't happen by accident. We have to defend it, fight for it, strengthen it, renew it. We have to prove that our model isn't a relic of our history; it's the single best way to revitalize the promise of our future."[21] This future is growing increasingly complex amid a rapidly evolving global security environment.

The assurance posture of the United States must be flexible enough to anticipate and respond to such an environment while maintaining a clear azimuth toward an overarching US vision of promoting free, open, and democratic societies. This requires consistent and in-depth consultation and dialogue with Allies and partners about the shifting regional and global security environment and how best to meet such challenges head on.

21. Joseph R. Biden Jr., remarks, 2021 Virtual Munich Security Conference, Washington, DC, February 19, 2021, https://www.whitehouse.gov/.

As the 2018 *Nuclear Posture Review* articulates,

> Similar to deterrence, there is no 'one size fits all' strategy for assurance. Assurance measures must continually adapt to the shifting requirements of a highly dynamic threat environment. Our assurance strategies are tailored to the differing requirements of the Euro-Atlantic and Asia-Pacific regions, accounting for the differing security environments, potential adversary capabilities, and varying alliance structures.[22]

What remains consistent across regions is the need for the United States to remain integrated with Allies and partners as part of an effective assurance posture.

Perpetual Integration

The idea of burden sharing is central to the concept of assurance. To be effective, assurance must be rooted in a shared commitment of both risks and responsibilities between states.[23] Only when a state has "skin in the game" will it be fully committed to an assurance relationship. Formal alliances and treaties are effective means by which such shared commitments are codified. To galvanize these alliances and treaties, the United States often demonstrates its assurance commitment through the integration of military forces.

Foreign basing, joint training, intelligence sharing, and foreign military sales are tangible examples of how the United States integrates military forces with Allies and partners to promote assurance. These activities are critically important and should be selectively maintained or enhanced to promote regional assurances vital to the national interests of the United States and its Allies and partners. While the US military cannot maintain a permanent worldwide presence—nor should it—the selective posturing of US military forces overseas sends an unequivocal message to Allies, partners, and potential adversaries alike. Such posturing provides a clear nexus with deterrence-by-denial strategies, which most scholars believe to be more effective than deterrence by punishment.[24]

Integration occurs at the strategic, operational, and tactical levels, all with profound effects. Strategically, the decision to posture US military forces overseas provides a crystal-clear signal about the importance of the inter-state relationship. Operationally, large-scale training exercises provide an opportunity for military forces to put strategy in motion and reinforce the need for, and benefit of, the robust capabilities

22. James N. Mattis, *Nuclear Posture Review* (Washington, DC: Office of the Secretary of Defense, February 2018), 35, https://media.defense.gov/.

23. David S. Yost, "Assurance and US Extended Deterrence in NATO," *International Affairs* 85, no. 4 (2009), https://doi.org/.

24. John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983); Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961); and Mazarr, *Understanding Deterrence*.

previously highlighted. Tactically, integration of US, Ally, and partner military forces forms a relational glue, promulgating assurance across fielded forces.

Collectively, perpetual integration, a compelling vision, past actions, and robust capabilities enrich the assurance relationship between the United States and its Allies and partners. Such assurance is a strategic imperative, yet assurance is not without its challenges.

Measures of Assurance

Given the complexity of understanding and applying assurance theory, what is the measure of effective assurance? Since assurance is ongoing, both a process and interminable product, it is meaningless to define an end state when assurance is complete. Yet there are tangible measures that serve as indicators as to the relative success of assurance: nonproliferation of nuclear weapons; an enduring trend toward a free, open, and democratic international order; and the positive perception of the Allies and partners for whom United States assurance efforts are intended.

Nuclear Nonproliferation

Nuclear nonproliferation is a fundamental reason why the United States provides extended nuclear deterrence to its Allies and partners. As the 2022 *Nuclear Posture Review* expresses,

> Part of our assurance to Allies and partners is a continued and strengthened commitment to arms control, nuclear nonproliferation, and nuclear risk reduction to improve collective security by reducing or constraining adversary capabilities.[25]

An Ally's or partner's confidence in the capability and will of the US nuclear deterrent is an important litmus test for the effectiveness of US assurance writ large. So as not to compound the increasingly complex twenty-first-century global security environment, maintaining current bounds of nuclear proliferation is a critically important objective in US national security strategy. As such, a principal measure of effective assurance is maintaining the status quo of nuclear versus nonnuclear states under the terms of the Treaty on the Non-Proliferation of Nuclear Weapons.

Democratic International Order

Another positive indicator of effective US assurance is global and regional trajectories toward a democratic system of governance. This includes the broad international affirmation of the basic human rights of a free, open, and democratic society.[26]

25. Austin, *Nuclear Posture Review*, 14.

26. See, for example, *Freedom in the World 2024*: *The Mounting Damage of Flawed Elections and Armed Conflict* (Washington, DC: Freedom House, 2024), https://freedomhouse.org/.

Perceptions of Allies and Partners

An Ally's or partner's confidence is arguably more important to assurance than the actual will and capability upon which such confidence is based. An Ally or partner state's actions, signaling, and messaging all provide indicators of how it perceives the effectiveness of US assurances. Yet to truly understand the perception of assurance from an Ally's or partner's perspective, enduring communication is required.

As former British Defence Minister Denis Healey argued in the 1960s, successful alliance relationships are a challenging endeavor.[27] Cultural differences, divergent strategic objectives, and language barriers contribute to the complexity of these relationships. Assurance will only succeed through clear, consistent, and collaborative communication and consultation, the bedrock of assurance.[28]

Challenges of Assurance

Healey famously articulated in his "Theorem" that "it takes only five per cent credibility of American retaliation to deter the Russians, but ninety-five per cent credibility to reassure the Europeans."[29] The practice of deterrence is a complex endeavor, but that of assurance is even more challenging.

Through five key principles, the National Research Council aptly summarizes the difficulties in characterizing, understanding, and achieving assurance. First, "Even at its simplest, assurance is complex." Specifically, the interpersonal and inter-state relationships necessary for effective assurance relationships are difficult to achieve and maintain, "because it involves building—and sustaining—trust and confidence among people, organizations, and countries."[30] Yet while cultivating an Ally's or partner's confidence in the will and capability of the US government may not be easy, it is worth pursuing. The complexity of assurance demands a perpetually robust commitment to ensure its effectiveness.

Second, just as there are varying types of assurance, "there is no single definition of credibility."[31] As one political scientist asserts, "There is an extensive literature on alliances, but very little in this literature explores what makes a state regard the commitment of an ally as credible."[32] Certainly, credibility of assurance is enhanced when such assurance is viewed from the vantage of the assured, when assurance guarantees are tailored to meet the dynamic needs of different states in different regions, and when such assurances are framed by a compelling vision of the value proposition they hold.

27. Denis Healey, *The Time of My Life* (London: W. W. Norton, 1989).
28. Austin, *Nuclear Posture Review*.
29. Healey, 243.
30. National Research Council, *Strategic Deterrence*, 30–31.
31. National Research Council, 30.
32. Knopf, "Varieties," 382.

Third, for all its benefits, "assurance can have negative side effects," and Ally or partner efforts may run counter to US interests.[33] In reference to the discussion of abandonment versus entrapment, states must persistently examine alliances, ensuring rewards outweigh risks. These potential negative side effects may be mitigated, to some extent, through clear and persistent communication between Allies and partners as well as through a certain degree of ambiguity, when appropriate, in messaging intent to potential adversaries. Drawing red lines should be the exception, not the rule, and must be reserved for clear existential threats against an alliance.

Fourth, "assurance involves all forms of national power."[34] Large, bureaucratic governments such as the United States struggle to effectively coordinate efforts both within and between departments. Since assurance is not, and should not be, a military-only effort, engagement across the interagency is paramount to the success of an integrated assurance approach. Enhancing collective understanding across the US government of what assurance is and why it is important should be a principal objective of any administration.

Fifth, in a dynamic global security environment, "What assures changes?"[35] In other words, how does the United States flex assurances to adapt to shifting security dilemmas? Deterrence is viewed by most as having a stabilizing effect. Assurance should do the same. Alliances and partnerships that are sustained through deliberate, ongoing assurance will be better postured to address rapid changes in global or regional security environments. As the 2010 *Quadrennial Defense Review* pronounces, "You can't surge trust."[36] Assurance must be sustained in perpetuity, treated as a strategic imperative.

Conclusion

Effective assurance is a strategic imperative in US security policy. Accordingly, a clear definition and understanding of assurance from the US perspective is vital. A theory of assurance understood as the process and interminable product of actions taken to enhance an Ally's or partner's confidence in securities provided through the capability and will of the US government is a firm step toward a cohesive US assurance policy. Understanding assurance as a process means actions undertaken are constant and comprised of numerous variables, including robust capabilities, past actions, a compelling vision, and perpetual integration. Finally, assurance, when properly understood, is assessed primarily from the perspective of the Ally or partner.

The force-multiplying effects of maintaining strong alliances are difficult to quantify, both from the perspective of allies and potential adversaries. But alliances clearly provide an asymmetric strategic advantage, and strong alliances are built and sustained through strong assurances.[37] Assurance must never be an afterthought to

33. National Research Council, *Strategic Deterrence*, 31.
34. National Research Council, 31.
35. National Research Council, 31.
36. *Quadrennial Defense Review*, 63.
37. Austin, *National Defense Strategy*.

deterrence; it must be studied, developed, and nurtured as the strategic imperative that it is. This article only scratches the surface of what should be a robust and enduring dialogue about what assurance is, what it is not, and why it matters. Æ

TENSIONS ON THE PENINSULA

Strategic Communication for the US-Northeast Asia Alliance System

Jessica Reneé Taylor

As the 2024 US presidential election approaches, provocations by North Korea are expected to increase in frequency and severity, increasing tensions on the Korean Peninsula. In deterring aggression amid a dearth of communication with Pyongyang, the US-Northeast Asia alliance system must reassess its strategic messaging in its responses to North Korea's provocations and in alliance military exercises while also avoiding inadvertently raising such tensions. At the same time, the United States must also strive for long-term policy stability relating to the Indo-Pacific region to avoid undermining deterrence and public confidence of alliance system member states.

As 2024 commenced, Democratic People's Republic of Korea (DPRK, or North Korea) experts debated whether North Korean leader Kim Jong-Un had decided to go to war.[1] Although the issue remains unsettled, based on historical data, the general consensus is that as the United States' 2024 presidential election nears, there will likely be an uptick in the frequency and severity of the DPRK's destabilizing military activities, often referred to as provocations.[2] The anticipated tense security environment on the Korean Peninsula mandates that the US-Northeast Asia alliance system—comprising the US bilateral alliances with the Republic of Korea (ROK, or South Korea) and Japan and the trilateral cooperation among the ROK, Japan, and the United States—review its strategic communication approach to North Korea with the goal of strengthening deterrence while simultaneously preventing an inadvertent escalation in tensions.

Potential for Conflict

While this author concurs with experts who argue it is unlikely that Kim Jong-Un has made the decision to go to war, the environment is ripe for North Korean armed

Major Jessica Taylor, USAFR, a nonresident fellow in the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security, has a master in foreign service from Georgetown University.

1. Robert L. Carlin and Siegfried S. Hecher, "Is Kim Jong Un Preparing for War?," 38 North, Henry L. Stimson Center, January 11, 2024, https://www.38north.org/.

2. Victor Cha and Andy Lim, "Slow Boil: What to Expect from the DPRK in 2024," Center for Strategic & International Studies (CSIS), January 16, 2024, https://www.csis.org/.

aggression below the threshold of full-scale conflict. For starters, the expected spate of provocation comes amid a lack of communication between Pyongyang and the alliance system, increasing the odds of inadvertent escalation, particularly as a result of a misinterpretation of the alliance system's intent.[3]

Second, Northeast Asia geopolitical tensions have been building and will likely continue unabated. Accompanying increased tensions have been what are perceived as tit-for-tat displays of advancing military capabilities and aggressive rhetoric between Pyongyang and the alliance system. The combination of these factors increases the risk of miscalculation in a situation that currently lacks avenues to seek clarification and that is marked by a persistent and pervasive lack of trust.

Complicating matters is that North Korea has been emboldened by its emerging security cooperation with Russia.[4] Amid outrage surrounding Russia's invasion of Ukraine, it is unlikely Moscow will pressure Pyongyang in line with the international community's concerns. Likewise, Beijing continues to enable Pyongyang's evasion of sanctions, raising questions about its willingness to rein in North Korea.[5]

Lastly, if North Korea displays a capability to hold the US homeland at risk with nuclear weapons, its leadership will be further emboldened to sow doubt in US security guarantees to South Korea and Japan. This could lead Pyongyang to calculate it can undertake limited armed aggression with impunity, believing the White House would be hesitant to respond.[6]

A Role for Strategic Communication

The US Department of Defense's concept of strategic communication stresses the importance of US government efforts in concert with its Allies to "engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of [its] interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power."[7] In line with this effort, the US-Northeast Asia alliance system must

3. Jeongmin Kim, "North Korea 'Blocking' Hotlines to South Korea, Unification Ministry Says," NK News, April 10, 2023, https://www.nknews.org/.

4. Hyonhee Shin, "North Korea Has Sent 6,700 Containers of Munitions to Russia, South Korea Says," Reuters, February 26, 2024, https://www.reuters.com/.

5. Jack Kim and Ju-min Park, "UN Members Concerned China, Russia Helping North Korea-US' Austin," Reuters, November 14, 2023, https://www.reuters.com/.

6. Sooyoung Oh, "What the US Midterm Results Mean for South Korea's Security and Economy: China Remains at Center of US Foreign Policy in East Asia, Leaving Little Room for Imagination on the Korean Peninsula," KoreaPro, November 14, 2022, https://koreapro.org/.

7. *Strategic Communication Joint Integrating Concept* (Washington, DC: US Department of Defense [DoD], October 2009), ii, https://www.jcs.mil/.

employ strategic communication to influence Pyongyang to avoid escalating geopolitical tensions.[8]

Yet the DoD's *Strategic Communication Joint Integrating Concept* stresses that messaging is only complete once the receiver has interpreted the message. Thus the challenge of effective communication is to anticipate what signal will trigger the desired interpretation.[9] Or as one analysis on strategic narratives notes, "military strategy rooted in elite politics and social dynamics is difficult to separate from strategic narratives," emphasizing that "military strategy forms a meaningful discourse that unites political narration, public understanding, and the application of military force to influence as adversary."[10]

Therein lies the crux of the matter: the US-Northeast Asia alliance system must avoid inadvertently escalating tensions with an opponent that refuses to communicate while simultaneously maintaining readiness to strengthen deterrence and reassure its public of its commitment to protect and defend it from aggression.

To address this conundrum, this article offers recommendations for the US-Northeast Asia alliance system to adjust its strategic communication in the areas of its strategic messaging surrounding DPRK provocations and US Ally and partner regional military exercises. This article also contends that the United States must seek long-term policy stability with regard to security guarantees for alliance system member states that supports the strategic messaging objectives of deterrence and public reassurance.

DPRK Provocations and Responses

Among the most pressing areas in need of strategic communication adjustments is the perceived US-Northeast Asia alliance system's military responses to the DPRK's provocations that fall below the threshold of armed aggression.

Some alliance system activities, such as missile tests, have occurred after a provocation by North Korea. As a result, media outlets in and outside South Korea report that these alliance activities add to tensions on the Korean peninsula. Yet DoD and State Department officials stress the alliance system's military maneuvers are scheduled well in advance and are not in direct response to any one such provocation. Instead, officials note that such prescheduled activities are intended to maintain military readiness.[11] But if the information space—including the media and policy forums—views the alliance system's activities as responses to individual DPRK provocations, how does North Korea perceive these activities? The uncertainty surrounding this question warrants an alliance system that intentionally works to avoid having its intent misinterpreted.

---

8. See, for example, David K. Berlo, *The Process of Communication: An Introduction to Theory and Practice* (New York: Holt, Rinehart and Winston, 1960), 11–12; and Carl Hovland, qtd. in Dick Lee, "Developing Effective Communications," Extension, University of Missouri, March 2022, https://extension.missouri.edu/.

9. DoD, *Strategic Communication.*

10. Nick Blas, "Beyond Storytelling: Operationalizing Strategic Narratives in Military Strategy," *Æther: A Journal of Strategic Airpower & Spacepower* 2, no. 1 (Spring 2023): 46, https://www.airuniversity.af.edu/.

11. Author interviews, off the record, with various senior DoD officials, April 8–18, 2024.

The ongoing spate of DPRK missile tests has the region on edge.[12] Pyongyang has unilaterally scrapped the entirety of the inter-Korean Comprehensive Military Agreement (CMA)—the 2018 military accord between it and Seoul intended to ease interstate tensions through implementing measures including ending military drills near the border and establishing no-fly zones—and has started to rebuild armed guard posts along the inter-Korean border, among other anti-CMA provisions, increasing tensions on the peninsula.[13] Kim Jong-Un has also rejected the maritime border between the Koreas, threatening to use force against vessels in this area.[14] North Korea's provocations have included firing artillery shells into the inter-Korean buffer zone and warning of "an unpredictable phase" on the Korean Peninsula, all in all increasing the odds of accidental armed exchange in the border region.[15]

As the author has written elsewhere, every provocation from North Korea is not deserving of a response. Instead, the alliance should acknowledge certain military exercises as normal and expected, adhere to a schedule of military exercises, and strengthen missile defense, thus focusing on maintaining readiness and deterrence and avoiding "the political pressure and pitfalls of continuing to respond to North Korea's antics."[16] If the alliance system's actions are being incorrectly perceived as in response to the DPRK's provocations, the alliance system should then take steps to correct the narrative in an effort to strengthen crisis stability.

Despite the US government's stance that the alliance does not respond to individual DPRK provocations, this claim is not consistent with historical data nor is it currently consistent across the alliance system. For instance, the South Korea–US alliance conducted exercises in response to a 2017 North Korean intercontinental ballistic missile launch.[17] Today, under the ROK's Yoon administration, Seoul has taken a more assertive stance by not only responding in kind but also often upping the ante to DPRK provocations.[18] Notably, so far under the Yoon administration, all of the DPRK's provocations have been below the threshold of an imminent armed threat.

North Korea and the international media have interpreted the US-Northeast Asia alliance system as flexing its military prowess in response to DPRK provocations. This

12. Karl Friedhoff, "Redeploying US Tactical Nukes May Not Go Far Enough for South Koreans," Korea Pro, October 22, 2022, https://koreapro.org/.

13. Soo-Hyang Choi, "North Korea Scraps Military Deal with South, Vows to Deploy New Weapons at Border," Reuters, November 22, 2023, https://www.reuters.com/.

14. Kim Eun-Jung, "South Korea Reaffirms Commitment to Defending de Facto Maritime Sea Border," Yonhap News Agency, February 15, 2024, https://en.yna.co.kr/.

15. Jeongmin Kim, "North Korea Launches Ballistic Missile after Criticizing US Extended Deterrence," NK News, November 17, 2022, https://www.nknews.org/.

16. Jessica Taylor, "Not Every North Korean Missile Needs a Response. South Korea and the US Should Focus More on Readiness and Deterrence," *New Atlanticist*, Atlantic Council, April 27, 2023, https://www.atlanticcouncil.org/.

17. Terri Moon Cronk, "U.S., South Korea Conduct Exercise Following North Korean Missile Launch," DoD, July 5, 2017, https://www.defense.gov/.

18. Ju-min Park and Soo-Hyang Choi, "North Korea Fires Artillery at Sea against South Military 'Gangsters,' " Reuters, January 5, 2024, https://www.reuters.com/.

perceived demonstration of military power has at times included shows of force through missile tests, live artillery fire, and the US deployment of nuclear-capable weapon systems within the vicinity of North Korea.[19]

Pyongyang's misperception of the alliance system's intent poses some risks. For instance, alliance activities in response to DPRK provocations increase the likelihood of misinterpretation of alliance signaling possibly due to an accident or a misreading of the alliance system's posture. For example, in October 2022, a missile crashed immediately after launch at a ROK military base during a joint drill by South Korea and the United States, which the ROK joint chiefs of staff reported as a response to the DPRK launching of intermediate-range ballistic missiles the day prior.[20] But what would have happened if this missile had instead landed in the vicinity of North Korea? The lack of communication with Pyongyang only further heightens the risk of a retaliatory response since the alliance would not be able to notify the North Korean government of the accident.

Observers note that what should be especially alarming for South Korea in possible scenarios like this is the DPRK's success in producing solid-fueled ballistic missiles, which reduce the time required for Pyongyang to prepare missile launches, increasing the chance of an immediate retaliation.[21] By thus responding to a provocation that did not pose an imminent threat, the alliance risked an escalation in tensions from a potential accidental misfire. But even absent an accident, militarily responding to such provocations still risks the misinterpretation of the alliance's messaging as an imminent attack on North Korea. As one scholar argues, the alliance cannot be sure its intended message of a show of force will be perceived as such by North Korea.[22]

North Korea's shifting nuclear employment doctrine only further complicates matters. Pyongyang now proclaims that military officials can use an "operation method" predetermined to conduct a nuclear strike "immediately" and "automatically" at a time of emergency where the core command leadership is under danger.[23] Observers note these changes all suggest North Korea now includes signs of "imminent attack" as conditions to use nuclear weapons, which marks a significant break from the DPRK 2013 law that only listed situations of second strike, not preemptive strikes.[24] This

19. William Gallo, "South Korea Embraces 'Tit for Tat' Approach to North's Provocations," VOA [Voice of America], January 6, 2023, https://www.voanews.com/; and Kim Gamel and Yoo Kyong Chang, "US Bombers, Jets Fly near N. Korean Border in Show of Force after Missile Test," *Stars and Stripes*, September 18, 2017, https://www.stripes.com/.

20. Lim Jeong-won, "Hyunmoo Missile Crashes in South Korean Base During Joint Drills," *Korean JoonAng Daily*, October 5, 2022, https://koreajoongangdaily.joins.com/.

21. Michael Cohen, "South Korea's new SLBMs are a signal to North Korea and the United States," NK News, September 21, 2021, https://www.nknews.org/.

22. Van Jackson, *On the Brink: Trump, Kim, and the Threat of Nuclear War* (Cambridge, UK: Cambridge University Press, 2018).

23. Colin Zwirko and Jeongmin Kim, "Kim Jong Un Says He Will 'Never Give Up' Nuclear Weapons, Rejects Future Talks," NK News, September 9, 2022, https://www.nknews.org/.

24. Zwirko and Kim.

further heightens the importance of the US-Northeast Asia alliance system avoiding military responses to provocations that do not pose an imminent threat.

Strategic Communication Recommendations

The alliance system should abstain from militarily responding to DPRK provocations that fall below the threshold of an immediate threat to the system's territories and populations.

Some observers argue the populations of alliance member states are the intended audience of alliance military responses to DPRK provocations, rather than North Korea itself. This is partially correct. Not only is the US-Northeast Asia alliance messaging focused on Pyongyang but it also aims to reassure the public of the system's political will and military ability to respond in a unified fashion in the event of armed aggression. Yet there are a couple of issues with this approach as it pertains to those provocations that do not pose an immediate armed threat.

For one, military responses to such provocations do not replicate the political or the military decision-making environment that alliance senior leaders would have to confront amid a crisis that did pose an immediate threat. For instance, in responding to a provocation, the White House likely does not assess that it risks a DPRK nuclear retaliatory strike on the US homeland by doing so.

Furthermore, there is little evidence that alliance military activities perceived as a reaction to DPRK provocations below the threshold of an immediate threat aid in reassuring the Allied public of the alliance system's will and capability to come to their defense if necessary. Instead, calls in South Korea, and to a much lesser extent Japan, for the states to obtain an indigenous nuclear weapon capability are increasing.[25] In addition, concerns have been raised among the ROK public and regional observers that the efforts to militarily respond to the DPRK's provocations are adding to tensions unnecessarily.[26] As a result, responding to such provocations not only fails to achieve the alliance's objectives but also risks inadvertently raising tensions and losing the international community's support for its actions.

The risks of inadvertent escalation significantly outweigh any benefits to a military response. Instead, the alliance system should focus on communicating that it can and will respond to armed aggression. And despite the frustrations with the DPRK's destabilizing behavior and the lack of progress in achieving lasting peace on the peninsula, the alliance system should continue to focus on diplomatic avenues to reach such a peace, reserving military avenues to respond to armed attacks.

25. Sayuri Romei, "Watching Ukraine, South Korea and Japan Eye Nuclear Weapons. Here's What the US Should Do," *Bulletin of the Atomic Scientists*, July 20, 2023, https://thebulletin.org/.

26. Jenny Town and James M. Lindsay, "North Korea's Nuclear Program with Jenny Town," April 11, 2023, in *President's Inbox*, produced by Ester Fang and Gabriel Sierra, Council on Foreign Relations, podcast, 35:02, https://thepresidentsinbox.podbean.com/.

The US-Northeast Asia alliance system should amplify its strategic communication ahead of and following its military activities.

To avoid the misinterpretation of its military readiness activities, the alliance system should increase its contact with the information environment surrounding such activities.[27] As previously mentioned, senior US government officials proclaim these activities are not conducted in response to any individual DPRK provocation.[28] This does not seem to be reflected in what amounts to unilateral activities from alliance members, as Seoul has demonstrated it will militarily respond to DPRK provocations.[29] Yet, while the alliance system's members at times may act unilaterally, the alliance system should still work collaboratively under shared objectives and be able to effectively communicate those objectives to avoid inadvertent conflict.

Former ROK senior government adviser Moon Chung-In asserts that South Korea has been more tepid in its responses to DPRK provocations into 2024 due to US pressure, demonstrating that such collaboration can be achieved.[30] Yet this is only a partial solution. To deter armed conflict, the alliance will still need to conduct military activities for maintaining military readiness and displaying the political will and military capability to act as a cohesive unit. But the alliance system should do so strategically and transparently, communicating the message that conducting military activities on the divided peninsula mandates special considerations due to the proximity and hermetic nature of North Korea.

Although those activities, such as missile readiness testing, may happen to occur following a DPRK provocation, the fact is that US missile test launches are scheduled months in advance, as this author has observed by personal experience as an active duty and reserve Air Force logistics readiness officer since 2005. For example, while the ROK/US Nuclear Consultative Group activities are strictly scheduled, they are perceived in the international media space as responses to individual DPRK provocations.[31]

To avoid misinterpretation of alliance activities, the activities should be briefed to the press well in advance and should be debriefed after the activities have concluded. In addition, the alliance system should specify in briefings that alliance activities are conducted to maintain readiness to credibly strengthen deterrence. In other words,

27. Joshua "Mule" Koslov and Kate McIlvaine, "The Truth about Messaging: Competition Requires Placing Information Objectives at the Center of All We Do," *Journal of Indo-Pacific Affairs* 4, no. 3 (Summer 2021), https://media.defense.gov/.

28. Author interviews with DoD officials, April 8–18, 2024.

29. Lim Jeong-won, "Hyunmoo Missile Crashes in South Korean Base during Joint Drills," *Korea JoongAng Daily*, October 5, 2022, https://koreajoongangdaily.joins.com/.

30. Moon Chung-In, "Rumbles of Thunder and Endangered Peace on the Korean Peninsula" Hybrid Program, January 31, 2024, produced by Korea Society and National Committee on American Foreign Policy, panel discussion and YouTube presentation, 1:15:24, audio and video, https://www.koreasociety.org/.

31. Jessica Taylor, "The US and South Korea Doubled Down on Ending the Kim Regime If It Uses Nuclear Weapons," in "Experts React: South Korea Embarks on a New Nuclear Era. How Will It Play Out?," *New Atlanticist*, July 19, 2023, https://www.atlanticcouncil.org/.

the alliance system should avoid being interpreted as heightening tensions and thereby possibly inadvertently heightening the threat perceptions of the alliance's public and of North Korea.

To this end, the alliance should also diversify its methods of briefing the information environment on its activities. For instance, apart from press briefings and joint statements, the alliance system should explain and clarify its activities in various print publications and on social media platforms in all three countries. In this way, it could also increase its reach to the public and the international community.

US-Northeast Asia Alliance System Exercises

In addition to its general military readiness activities, the US-Northeast Asia alliance system should be wary of inadvertently communicating hostile intent in alliance system military exercises.

The alliance system's practices in support of military readiness add credibility to strategic messaging that it has the military capability to impose unacceptable costs in response to DPRK aggression. Thereby one of the strategic messaging goals of maintaining military readiness is to deter armed aggression by hopefully influencing the DPRK's strategic decision-making calculus. Furthermore, the alliance system's exercises also display to the public that its militaries are prepared to respond if deterrence fails. But the proximity of North Korea mandates that the alliance conduct its drills in a manner that avoids messaging offensive hostile intent.

Currently, all members of the alliance system support greater security cooperation with the treaty alliances and trilaterally. This is a monumental shift from recent years. As a result of efforts to improve inter-Korean relations amid a concurrent deterioration of South Korea–Japan relations, US-Northeast Asia alliance system exercises were significantly scaled back, canceled, or nonexistent from 2018 to 2022, as in the case of trilateral cooperation during the Moon and Trump administrations.[32]

Scaled-down military theater exercises meant that additional personnel and military assets were not deployed to the Korean Peninsula.[33] In addition, at times, the Trump administration unilaterally threatened to cancel or outright canceled theater-level joint ROK-US annual exercises, citing the exercises' costs or expressing the hope of using them as bargaining chips to persuade North Korea to align with US interests.[34]

With the change in administrations in Seoul, Tokyo, and Washington, however, there has been greater alignment in DPRK threat perception.[35] This has come with

32. Thomas Spoehr, "Why Ending U.S.-South Korea Joint Exercises Was the Wrong Move," Heritage Foundation, May 3, 2019, https://www.heritage.org/.

33. Troy Stangarone, "South Korea, US Return to Large-Scale Military Drills," *Diplomat*, August 25, 2022, https://thediplomat.com/.

34. Eric Schmitt, "Pentagon and Seoul Surprised by Trump Pledge to Halt Military Exercises," *New York Times*, June 12, 2018, https://www.nytimes.com/.

35. Frank Aum and Mirna Galic, "What's behind Japan and South Korea's Latest Attempt to Mend Ties?," United States Institute of Peace, March 21, 2023, https://www.usip.org/.

multiple efforts to strengthen the cooperation and military readiness of the alliance system amid North Korea's evolving missile and nuclear capabilities. Notably, the alliance system has increased the frequency and level of joint exercises and efforts toward institutionalizing the real-time sharing of DPRK missile data.[36] And in 2023, the ROK-US alliance, in acknowledging its 70-year partnership, held what it categorized "as the largest exercises" ever to include its largest live-fire joint drill near the demilitarized zone.[37]

The shift in frequency and scale of alliance system's exercises has been a drastic pendulum swing from the previous administration. At times such activities have been reported as contributing to an increase in tensions with North Korea.[38] Furthermore, attempts within the alliance system to return to historical exercise schedules and levels have often been perceived as responses to DPRK provocations, especially as North Korea frequently launches missiles around such military exercises as a display of discontent.[39]

As US-Northeast Asia alliance exercises have long been a source of contention with North Korea, historically alliance system leaders have used exercises as carrots and/or sticks, depending on the administration in office, in an effort to compel North Korea to acquiesce to the interests of regional stability.[40] This comes as Pyongyang condemns such exercises, asserting that they are a rehearsal for a future invasion of North Korea.[41] Still, the alliance system insists its exercises are defensive.[42]

But whether or not North Korea is concerned about an invasion, the alliance system cannot be absolutely certain. On the contrary, what is certain is that Russia has displayed through its 2022 full-scale invasion of Ukraine that a neighboring state can operate under the guise of a military exercise to stage for an invasion.[43] And thus the DPRK may actually interpret alliance drills as an invasion threat. The lack of certainty increases the importance of ensuring the strategic communication projected from these exercises aims to avoid misinterpretation of intent, particularly with the

36. DoD, "United States-Japan-Republic of Korea Trilateral Ministerial Joint Press Statement," press release, December 19, 2023, https://www.defense.gov/; and Lee Hyon-jin, "S. Korea, US Plan Largest Military Drill to Commemorate Alliance," *Korea Times*, March 23, 2023, https://www.koreatimes.co.kr/.

37. Lee.

38. Taylor, "North Korean Missile."

39. Taylor.

40. Hyonhee Shin, "North Korea Criticizes US, South Korea Military Drills As 'Nuclear Blackmail,' " Reuters, May 18, 2023, https://www.reuters.com/; and Robert Collins, "A Brief History of the US-ROK Combined Military Exercises," 38 North, February 26, 2014, https://www.38north.org/.

40. Hyung-Jin Kim, "North Korea's Kim Calls for Stronger War Fighting Capabilities against the US and South Korea," AP, March 6, 2024, https://apnews.com/.

41. Kim.

42. Jared Gans, "North Korea Warns US, South Korea Military Drills Escalate Tension to 'Brink of a Nuclear War,' " *Hill*, April 6, 2023, https://thehill.com/.

43. Alex Horton et al., "Launch of Russia Military Drills Stokes Fears of Preparations for Attack on Ukraine, As Diplomatic Sparring Continues," *Washington Post*, February 10, 2022, https://www.washingtonpost.com/.

expectation that North Korea is likely to carry out provocations and military exercises near inter-Korean border areas as the 2024 US presidential election approaches.

Strategic Communication Recommendations

While the alliance should conduct military exercises, it should do so in a manner that prevents inadvertent escalation while simultaneously strengthening military readiness, deterrence, and public reassurance. To these ends the alliance system's strategic communication approach to military exercises should implement certain improvements.

The US-Northeast Asia alliance system should refrain from conducting exercises in the inter-Korean border areas.

Military exercises conducted in the vicinity of the inter-Korean border areas, particularly those that include live artillery fire, needlessly raise tensions and risk unintended escalation due to an accident or misinterpretation of strategic messaging. Spring 2024's theater-level ROK-US Freedom Shield exercise started amid ROK public concern that the alliance system was exacerbating the tensions on the Korean Peninsula.[44] Aiming to quell concern, ROK joint chiefs of staff noted that none of the 48 military drills being held as part of the exercise would be conducted near the inter-Korean border areas.[45] The alliance system should make this a permanent practice.

Rather than hold exercises at exercise facilities along the border, the alliance system should instead simulate inter-Korean border areas in alternate locations, which will still allow it to strengthen deterrence through the maintenance of military readiness.[46] Furthermore, member states of the US-Northeast Asia alliance system would be more successful in maintaining their public's confidence that the alliance system as a whole is refraining from unnecessarily adding to tensions. This will increasingly be important as North Korea is expected to hold more military activities near the inter-Korean border areas following its unilateral scrapping of the inter-Korean CMA.[47]

The alliance system should avoid using military exercises as a punishment or as a bargaining chip.

The alliance could avoid misinterpretations of messaging surrounding the system's exercises by only utilizing exercises for military readiness purposes. The use of exercises as a punishment undermines messaging that the exercises are purely defensive.

---

44. Nick Schifrin et al., "US, South Korea Conduct Military Exercises As North Korea Ramps Up Missile Testing," PBS NewsHour, March 21, 2023, video and transcript, 6:04, https://www.pbs.org/.

45. Chae Yun-hwan, "S. Korea, U.S. Begin Key Annual Military Drills Amid N.K. Threats," Yonhap News Agency, March 4, 2024, https://en.yna.co.kr/.

46. Author interviews with DoD officials.

47. Soyoung Kim, "What Was in the Now-Scrapped Inter-Korea Military Agreement," *Diplomat*, November 28, 2023, https://thediplomat.com/.

In addition, exercises perceived as punishing North Korea are publicly seen as needlessly adding to an already tense environment.[48]

At the same time, the alliance system should refrain from offering alliance exercises as bargaining chips. Doing so undermines military readiness and risks alliance cohesion and therefore undercuts deterrence.[49] For example, amid the scaled-down alliance system drills during the previous administrations in South Korea, the United States, and Japan, North Korea maintained its exercise cycle while also advancing its nuclear and missile capabilities.[50] As a result, the alliance system under the current government administrations felt compelled to quickly return to a regular exercise schedule in an effort to strengthen deterrence and the public's confidence amid concerns that both had decreased in recent years.

Furthermore, the drastic policy shift from postponing or outrightly canceling exercises to reinstating them with an increase in frequency and scale creates a whiplash effect on the Korean Peninsula. This not only risks unintentionally heightening the DPRK's threat perception of a coming shift in alliance intentions but also may be perceived by the public and international community as unnecessarily raising tensions between the Koreas. As such the US-Northeast Asia alliance system should maintain a regular exercise schedule to credibly message its military readiness to respond to DPRK-armed aggression. Doing so also should aid in preventing the perception that alliance exercises are used to punish the DPRK.

Overall, by implementing these measures surrounding the alliance system's responses to DPRK provocations and the system's military exercises, the system will be able to maintain its military readiness and strengthen deterrence and public confidence without risking regional stability.

US Intent

The reality of the US political system can challenge sustained alliance system strategic communication related to political willingness and military capability to respond to threats to other members of the alliance system. Resulting alliance mismanagement could undermine deterrence, thus risking the DPRK calculating it could conduct even limited armed aggression with impunity. For instance, there is concern that North Korea will soon move again to carry out limited armed aggression akin to its 2010 response against South Korea.[51] This scenario harkens back to the Korean War, when

48. Jenny Town, "Has Conflict on the Korean Peninsula Become Inevitable," Arms Control Association, March 2024, https://www.armscontrol.org/.

49. Chung Min Lee and Kathryn Botto, eds., *Korea Net Assessment: Politicized Security and Unchanging Strategic Realities* (Washington, DC: Carnegie Endowment for International Peace, March 18, 2020), https://carnegieendowment.org/.

50. Julia Masterson, "UN Experts See North Korean Nuclear Gain," Arms Control Association, September 2020, https://www.armscontrol.org/.

51. CNN Wire Staff, "North Korea Strike, South Korean Leader Threatens 'Retaliation,' " CNN, November 24, 2010, https://www.cnn.com/.

Kim Il Sung observed the US military drawdown from South Korea and the US government's proclaiming the South Korea was out of the US defense perimeter as indications that the United States would not come to its defense.[52] Some DPRK experts even warn North Korea may attempt a quick seizure of ROK territory.[53]

While the alliance system has made great strides in boosting security cooperation, those efforts may be in vain, absent credible indicators of enduring political support of the alliance's military aims, namely US security guarantees.[54] Discourse surrounding concerns of alliance system cohesion usually focuses on questions of whether the United States would be willing to risk its own security to come to the aid of its Allies. This debate intensifies as North Korea comes closer to a nuclear-strike capability against the US homeland, in an effort to deter the United States from responding to a limited DPRK attack against South Korea. A failure to adequately message the endurance of alliance cohesion and particularly the US commitment to its security guarantees poses risks to deterrence and public reassurance.

Furthermore, a failure to credibly message the endurance of alliance cohesion risks undermining the public confidence that the alliance has the political will and military capability to respond to armed aggression should deterrence fail. In particular, different US administrations over the years have pushed to reduce US military presence in Ally and partner countries, assessing that lessening the threat posed to US interests means decreasing the number of US citizens in harm's way.[55]

Concern over the endurance of the US commitment is complicated by North Korea's pursuit of its nuclear capabilities and the Russian full-scale invasion of Ukraine, which has incited ROK citizens' desire for their own indigenous nuclear weapon capability. If met, this will likely further destabilize Northeast Asia through the heightened threat perception of all of South Korea's neighbors.[56]

Thus the United States has been working with South Korea toward better consultation on nuclear threats, and there has been an increase in trilateral security cooperation toward DPRK missile threats.[57] In addition there are nascent indications that the nuclear consultation could eventually include Japan.[58] Efforts in these areas will be in vain if there is not a sustained political commitment to current US strategic messaging,

52. Thomas J. Christensen, Worse Than a Monolith: Alliance Politics and Problems of Coercive Diplomacy in Asia, Core Textbook ed. (Princeton: Princeton University Press, 2011).

53. "Predicting 2024: Why the Writing Is on the Wall for an Inter-Korean Border Clash," NK Pro, January 10, 2024, https://www.nknews.org/.

54. White House, "The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States," press release, August 18, 2023, https://www.whitehouse.gov/.

55. Veronica Stracqualursi, "Trump Apparently Threatens to Withdraw US Troops from South Korea over Trade," CNN, March 16, 2018, https://www.cnn.com/.

56. Foster Klug, "South Koreans Want Their Own Nukes. That Could Roil One of the World's Most Dangerous Regions," AP, November 29, 2023, https://apnews.com/.

57. White House, "Camp David."

58. Ji Da-gyum, "S. Korea Open to Japan Joining Nuclear Consultative Group: Ex-Security Advisor," *Korea Herald*, February 13, 2024, https://m.koreaherald.com/.

even across different presidential administrations, regarding an enduring commitment to security guarantees in the region.[59]

Congressional and administration internal strife has, among other things, delayed military aid to US partners embroiled in armed conflicts, most recently to Ukraine and to Israel. Decisionmakers persistently hamstring policy for the sake of unrelated policy issues.[60] Some may be quick to assume that the United States would approach armed aggression against US treaty allies differently. But it is unknown whether North Korea views the US approach to treaty allies and nontreaty partners differently. Unfortunately, absent acknowledgement by the opponent, deterrence effectiveness can only be measured if it fails.

Moreover, the almost 30-year congressional preference for continuing resolutions—1997 was the last year without at least one—has exacerbated the tendency toward sustained impasse on important issues.[61] Defense Secretary Lloyd J. Austin has warned how the constant threat of extending these resolutions impacts military readiness.[62] Michele Flourney, former US under secretary of defense for policy, has consistently noted that operating on continuing resolutions prevents the United States from modernizing outdated and inefficient systems and forestalls the funding of new defense articles to meet emerging threats.[63] North Korea and US Allies take note, thereby undermining deterrence and public reassurance.

In particular, policy instability hampers the US-Northeast Asia alliance system's messaging efforts that it has the political will and military capability to respond to armed aggression. Prioritizing US political party interests over national security interests risks eroding deterrence and public reassurance and weakens the long-term credibility of US security guarantees.

Conclusion

The US-Northeast Asia alliance system's leadership has not provided any indication that it assesses North Korea intends to go to war. Yet, decisionmakers cannot rule out an inadvertent escalation in tensions, nor can they rule out North Korea's calculations that it could carry out even limited armed aggression with impunity.

---

59. Kate Sullivan, "Trump Says He Would Encourage Russia to 'Do Whatever the Hell They Want' to Any NATO Country That Doesn't Pay Enough," CNN, February 11, 2024, https://www.cnn.com/.

60. Morgan Chalfant, "McConnell Threatens Semiconductor Bill, Prompting White House Rebuke," *Hill*, June 30, 2022, https://thehill.com/; and Stephen Groves et al., "Senate Republicans Resist Advancing on Border Policy Bills, Leaving Aid for Ukraine in Doubt," AP, February 7, 2024, https://apnews.com/.

61. James V. Saturno et al., *Continuing Resolutions: Overview of Components and Practices*, R46595 (Washington, DC: Congressional Research Service, May 16, 2023), introduction, https://crsreports.congress.gov/.

62. Secretary of Defense Lloyd J. Austin to Senate Majority Leader Charles Schumer, letter, November 27, 2022, https://www.airandspaceforces.com/.

63. Kedar Pavgi, "Former Defense Official Calls Congressional Paralysis a Threat," *Government Executive*, October 17, 2012, https://www.govexec.com/.

The geopolitical environment in Northeast Asia is particularly tense. North Korea has severed communication channels with the US-Northeast Asia alliance system, which means direct communication amid a crisis to prevent escalation may be unlikely. In addition, considering the seeming lack of avenues for great power cooperation with North Korea, the alliance system's strategic communication is increasingly important to maintaining crisis stability.

With limited avenues to impact North Korea's strategic calculus, the alliance system should avoid responding to provocations that are not an immediate threat, and should look for ways to more clearly message North Korea and the international community regarding routine alliance system military exercises. Furthermore, while the return to full-scale exercises and trilateral security cooperation aids in strengthening deterrence, it should be done in a manner that improves military readiness without risking inadvertent escalation.

Lastly, members of both parties in Congress and the presidential candidates should prioritize a consistent message of unflinching, meaningful support to the alliance system. Failing to do so risks undermining deterrence and public confidence in US security guarantees. Æ

POLICY CHANGE TAKES FLIGHT

The Department of the Air Force Women's Initiatives Team

Kelly Atkinson

How does policy change occur within an institution? This article presents a framework to examine agents of policy change as key mechanisms for understanding institutional transformation. A case study evaluation of the Department of the Air Force Women's Initiatives Team—an all-volunteer effort that has generated policy changes addressing military uniform standards, aircraft design, reproductive healthcare access, and parental leave—explores how gender policy change in the Department of the Air Force has unfolded over the past decade. By utilizing ethnographic and policy research, this article traces the individual and group dynamics shaping the team's activities as well as the collective action challenges facing such changes within the department, with implications for institutions in general.

How do institutions change over time?[1] This question lies at the heart of political and sociological study, with these disciplines often focusing on economic trade-offs and historical analysis to solve this puzzle. Yet as policy change efforts within and across institutions become more prevalent, the traditional economic and historical lenses are limited in their ability to engage complex individual and group dynamics that lie at the heart of institutional longevity and change.

Addressing this knowledge gap, this article presents a new framework to analyze institutional change. This framework assesses the interaction between groups interested in policy change, those unwilling or unable to support change, and the levels of interest and power that shape not only motivations but also abilities to overcome collective action

Lieutenant Colonel Kelly Atkinson, USAFR, PhD, is a political scientist with the RAND Corporation and a future operations planner for admissions at the US Air Force Academy.

1. The author is grateful to the members of the Department of the Air Force (DAF) Women's Initiatives Team (WIT) for sharing their data on efforts and outcomes in support of this article and for their continued leadership of gender policy change across the Department. The author appreciates feedback received on an early draft of this piece from Gender & Politics panel reviewers at the April 2024 Midwest Political Science Association Conference. Thank you as well to the thoughtful peer reviewers and editors of this journal for improving this article through your comments and suggestions. The views, opinions, findings, conclusions, and recommendations contained herein are the author's alone and not those of the RAND Corporation or its research sponsors, clients, or grantors.

problems. The theoretical foundation for this new framework derives from feminist analyses of institutions and power, which point to the critical importance of understanding individual-level dynamics in order to comprehend the complexity of institutions and institutional change.[2] Applying this framework to a case study of the Department of the Air Force's (DAF) Women's Initiatives Team (WIT) reveals that individual and group-level dynamics within institutions provide insights into the nature of agent-driven incremental change that ultimately transforms institutions from within.

Theoretical Foundations

The disciplines of political science and sociology maintain well-established foci on institutions, or "the rules of the game in a society . . . the humanly devised constraints that shape human interaction."[3] Institutions consist of the set of rules and norms guiding behavior among individual actors, or agents, within the system. From a constructivist viewpoint, people create institutions. They are not stagnant, permanent fixtures; instead institutions are produced by people, for people.[4] A feminist analytical approach, which pays attention to hierarchies of power, approaches institutions as ultimately constructed systems that shape agents' access to power, empowering some populations while disempowering others.[5]

At the same time, as populations enter and leave institutions, they indelibly change the nature of those institutions by reshaping power distributed within and beyond them. Understanding these networks of power internal to institutions themselves sheds light on the function and efficacy of those institutions. Additionally, understanding how institutions change reveals how these networks of power shift and transform over time. Ultimately, "institutional change shapes the way societies evolve through time and hence is the key to understanding historical change."[6]

One way to understand institutional change is through path-dependent analysis.[7] According to one sociologist, "the identification of path dependence . . . involves both tracing a given outcome back to a particular set of historical events, and showing how

2. See J. Ann Tickner, *Gender in International Relations: Feminist Perspectives on Achieving Global Security* (New York: Columbia University Press, 1992); Cynthia Enloe, *Bananas, Beaches and Bases: Making Feminist Sense of International Politics* (Berkeley: University of California Press, 2014); and Carol Cohn, "Sex and Death in the Rational World of Defense Intellectuals," *Signs: Journal of Women in Culture and Society* 12, no. 4 (1987).

3. Douglass C. North, *Institutions, Institutional Change and Economic Performance*, Political Economy of Institutions and Decisions (Cambridge, UK: Cambridge University Press, 1990), 3; and James Mahoney and Kathleen Thelen, eds., *Explaining Institutional Change: Ambiguity, Agency, and Power* (New York: Cambridge University Press, 2009).

4. Alexander Wendt, "Constructing International Politics," *International Security* 20, no. 1 (1995).

5. J. Ann Tickner, "Feminism Meets International Relations: Some Methodological Issues," *Feminist Methodologies for International Relations* 41 (2006).

6. North, *Institutions*, 3.

7. Jacob Torfing, "Rethinking Path Dependence in Public Policy Research," *Critical Policy Studies* 3, no. 1 (2009).

these events are themselves contingent occurrences that cannot be explained on the basis of prior historical conditions."[8] As a qualitative methodological approach, path-dependent analysis reveals the timing and sequence behind certain events that, linked together, produce particular outcomes. Sequences may be self-reinforcing or reactive, and these path-dependent sequences produce inertia: "Once processes are set into motion and begin tracking a particular outcome, these processes tend to stay in motion and continue to track this outcome."[9]

Considering institutions, conceptualized here to be constructed systems that shape agent access to power, inertia becomes a mechanism for self-preservation. An institution set into motion will reproduce the structures, rules, and norms that keep the institution strong. Agents within the institution who benefit from these rules and norms—that is, those who maintain and grow their power within the system—become less inclined to change the institution that rewards their participation. As time passes it becomes more difficult to disrupt these established processes, and institutional change grows difficult.

Critical junctures offer a window into how institutional change occurs and represent "the adoption of a particular institutional arrangement from among two or more alternatives."[10] Critical junctures often reflect shocks to an institutional system, marking a scenario in which an institution must progress down one road while rejecting alternative options. These critical junctures, such as the terrorist attacks of September 11, 2001, can often appear obvious when viewed through the lens of historical analysis.[11]

Yet not all critical junctures are as striking as black smoke against a clear blue sky. Sometimes, critical junctures leading to institutional change reflect the painstaking work of agents, slowly reshaping the power structures within an institution so steadfastly that alternative arrangements are no longer viable. In order to understand the quotidian mechanisms through which institutions change over time, research must consider the foundation of institutions themselves—the agents within the system.

Toward a Model of Agency within Institutions

When considering agents acting within institutions, where institutions are systems of constraints that coordinate behavior and agency while regulating power, a rational actor framework offers certain theoretical contributions.[12] Within this framework, individuals navigate a system of incentives and disincentives to maximize their own

8. James Mahoney, "Path Dependence in Historical Sociology," *Theory and Society* 29, no. 4 (2000): 507–8.

9. Mahoney, 511.

10. Mahoney, 513.

11. Sidney Tarrow, "'The World Changed Today!' Can We Recognize Critical Junctures When We See Them?," *Qualitative and Multi-Method Research* 15, no. 1 (2017): 9–11.

12. North, *Institutions*.

benefit.[13] This behavior becomes complicated when individuals join together in groups but may possess conflicting interests. This leads to the logic of collective action and free-rider problems: if people work together to achieve a common good, then others who did not pay the cost for the good might still benefit from the outcome, thus disincentivizing a group to pursue achieving the common good at all.[14]

Of course, the rational actor framework and associated collective action logic are not without critique.[15] One feminist analysis has argued that adopting a rational actor framework imbues all agents with an economic scale of priorities reflecting patriarchal Western values.[16] Further, this approach may ignore other bodies of knowledge while conflating economic self-interest with rationality and thus, to a logical conclusion, humanity.[17] Moreover, reducing agents to rational actors ignores the visceral lived experiences of individuals and groups engaged in institutional change. The identity politics, contentious group dynamics, negotiations and trade-offs, shared victories and losses, and often-literal blood, sweat, and tears shaping policy change efforts remain invisible when ignored by traditional rational actor models.[18]

Still, the rational actor framework and associated collective action logic are central to disciplines of political science and sociology—so how can they evolve to produce new modes of understanding institutional change? This article posits that the rational actor and collective action frameworks may enable the productive study of change within institutions only when augmented with path-dependent analyses that evaluate individual and group dynamics among agents within the institution.

In this approach, rational actor dynamics do not solely reflect decisions between incentives and disincentives. Rather, factors influencing decision-making within institutions also include historical context, individual and group identity, and networks of power. Without understanding these dynamics, any evaluation of agents overcoming the collective action problem to initiate institutional change remains incomplete.

13. Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, MA: Harvard University Press, 1965).

14. Elinor Ostrom, "Collective Action and the Evolution of Social Norms," *Journal of Economic Perspectives* 14, no. 3 (2000).

15. Paula England, "A Feminist Critique of Rational-Choice Theories: Implications for Sociology," *American Sociologist* 20, no. 1 (1989).

16. Val Plumwood, "The Politics of Reason: Towards a Feminist Logic," *Australasian Journal of Philosophy* 71, no. 4 (1993).

17. Joyce Green, ed. *Making Space for Indigenous Feminism*, 2nd ed. (Black Point, Nova Scotia: Fernwood Publishing, 2020).

18. See Raymond Caldwell, *Agency and Change: Rethinking Change Agency in Organizations* (Abingdon, UK: Routledge, 2006); and Jean Hartley, John Benington, and Peter Binns, "Researching the Roles of Internal-Change Agents in the Management of Organizational Change," *British Journal of Management* 8, no. 1 (1997).

Conceptualizing Agents of Institutional Change

To understand the full scope of how institutional change occurs, the mechanisms through which individuals and groups navigate and change the norms and rules, or policies, of their institution merit scrutiny. At the heart of these negotiations lies power: Who has it, who seeks it, and who wields it? Moreover, who desires to change policy—and thus the distribution of power—and whose interests lie in maintaining the status quo? The new framework presented below integrates feminist paradigms to understand power with an evaluation of institutions and organizational change.[19]

Figure 1 details a new framework to categorize the nexus of power and interest across an institution's population. In this model, an institution represents a discrete unit with its own internal policies. These policies structure the norms and rules constraining behavior and shaping incentives in the system. Agents are members of the institution, and the institution endures over time without experiencing severe shocks generating critical junctures. Given these scoping conditions, the model categorizes the agents who prove capable of changing the institution's policies and, thus, the institution itself. This model does not aim to reflect every agent within an institution but rather to categorize the individuals and groups involved in policy change dynamics.

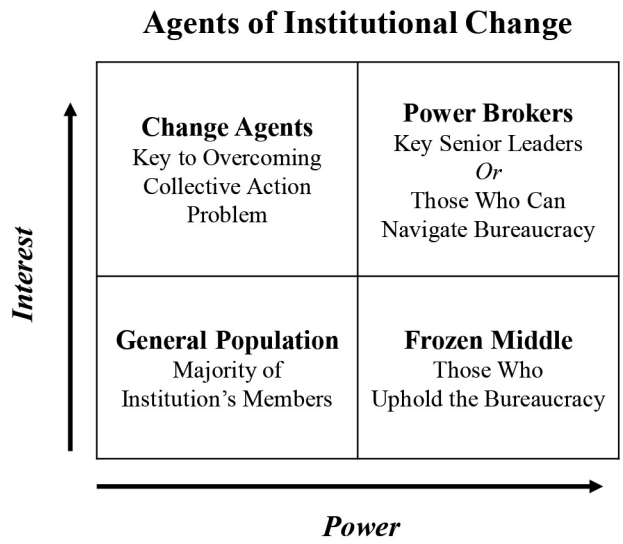

Figure 1. A framework for agents of institutional change

The model operates along the axes of power and interest, where power represents an agent's power in the institution and interest represents the agent's interest in

19. See Joan Acker, "Gender and Organizations," *Handbook of the Sociology of Gender* (Dordrecht, Netherlands: Springer Science + Business Media, 2006); and Marta B. Calás et al., "From the 'Woman's Point Of View': Feminist Approaches to Organization Studies," *Studying Organization: Theory and Method* 212 (1999): 251.

changing policy in the institution. The general population consists of the majority of the institution's members: they have low to moderate power and minimal interest in changing policy. Change agents are those who have low to moderate power but possess a high level of interest in changing policy. Additionally, this model simplifies concepts for instructional design and therefore does not capture the myriad motivations and dynamics involved in situations of institutional change.

As more people gain interest in policy change and subsequently transition from general population to change agents, the change agents become more likely to overcome collective action challenges in their efforts to change policy since more individuals are invested in change outcomes, thus reducing the free-rider problem.

Power brokers facilitate policy change—they possess high levels of power in the institution and a high level of interest in changing policy. These agents may be key senior leaders who possess positional power, or they may include agents who understand the institution keenly and can therefore navigate the constraints of the system. In either case, power brokers partner with change agents to foster policy change.

Finally, the frozen middle represents those with high levels of power in the institution but low levels of interest in changing policy. In some cases, the frozen middle has low interest in institutional change since they are overtasked and underresourced, compelled to stay within their roles through time and task constraints. They have no interest in policy change because they have no time available to consider alternatives. In other cases, the frozen middle wants to uphold the bureaucracy and its associated administrative constraints for ideological reasons: they gained power through the institution's existing structures, and therefore they oppose changes to the system that benefited them.

In either case, the frozen middle slows down or even thwarts attempts by change agents to transform institutional policy. Power brokers, particularly key senior leaders, may overrule the frozen middle in some cases, but often the frozen middle is so deeply entrenched in the institution's power structures that they can withstand power broker efforts.

Considering this model and its internal mechanisms, how do these dynamics play out in a real-world example? To illustrate the model, this article presents a short case study of the US Air Force Women's Initiatives Team. This evaluation is based upon the author's experience working with and observing the WIT for over six years. Such ethnographic assessment, although shaped by the subjectivity of participant observation, still proves valuable when conceptualizing and illuminating the internal mechanisms of an opaque institution such as the US military.[20]

Case Study: US Air Force Women's Initiatives Team

The US Air Force Women's Initiatives Team provides a unique example of a coordinated effort to change policy in an institution, led by members of the institution itself.

20. Richard Handler, *Critics against Culture: Anthropological Observers of Mass Society* (Madison: University of Wisconsin Press, 2005).

The WIT is one subset of a broader barrier analysis working group structure operating across the Department of Defense. The Department of the Air Force chartered its barrier analysis working group in 2008, in accordance with Management Directive 715 issued by the US Equal Employment Opportunity Commission in 2003. According to this directive, the purpose of barrier analysis is "an investigation of anomalies, or triggers, found in an agency's employment-related policies, procedures, practices, and conditions." The investigation aims "to identify the root cause(s) of those anomalies" and develop "plans for eliminating the barriers."[21]

The Women's Initiatives Team was established in 2008, and as of 2021, the DAF has formally established seven teams within the structure of the barrier analysis working group:[22]

- Black/African American Employment Strategy Team
- Disability Action Team
- Hispanic Empowerment and Advancement Team
- Indigenous Nations Equality Team
- LGBTQ Initiative Team
- Pacific Islander/Asian American Community Team
- Women's Initiatives Team

As a team within the working group structure, the WIT's mission is to identify barriers to women's service in the DAF and Defense Department that influence and impact women's propensity to serve and advocate to eliminate those barriers through policy change. The WIT is run by volunteers and maintains six lines of effort, as of 2024:

- Childcare Programs, Policies, and Entitlements
- Pregnancy Discrimination and Maternal Bias
- Female-Specialized Healthcare
- Outreach and Recognition
- DAF Development
- One Size Does Not Fit All (Anthropometrics)

The WIT is perhaps the most widely recognized barrier analysis working group within the Department of the Air Force. This is in large part due to a 2021 WIT-led

21. "Instructions to Federal Agencies for EEO MD-715," US Equal Employment Opportunity Commission, accessed March 13, 2024, https://www.eeoc.gov/.

22. Secretary of the Air Force Public Affairs (SecAF PA), "Department of the Air Force Creates Two New Barrier Analysis Working Groups for LGBTQ, Indigenous Nation Members," US Air Force (USAF), April 26, 2021, https://www.af.mil/.

policy change to update hair standards for women in the Air Force and Space Force.[23] The visibility of this change, which enabled DAF women to wear their hair in ponytails or braids in addition to the traditional bun, marked a tangible outcome of policy change efforts that often remain hidden within bureaucratic structures.[24] A comprehensive list of WIT policy change efforts is included below:

Table 1. DAF WIT policy change accomplishments[25]

2024
• Update to Medical Standards Directory implementing refined stature standards for career enlisted aviators, based upon anthropometric study utilizing representative measurements
• Update to DAF Instruction (DAFI) 63-101 *Anthropometric Design Specifications* directing that such specifications must accommodate body sizes of at least the central 95 percent of the US recruiting population, including all races and genders
• Authorization of women's wear of mess dress slacks in DAFI 36-2903, *Dress and Personal Appearance of DAF Personnel*
• Authorization of commercial cold weather outerwear for pregnant Airmen and Guardians
• Joint travel regulation authorization for five-year pilot program of travel reimbursement for childcare support from a family or friend during a military move
• Protection of parental leave while enrolled in professional military education (PME)
• Implementation of flexible spending accounts for service members
2023
• Reimbursement of meal fees as part of childcare fee assistance
• US Special Operations Command policy update to authorize Bluetooth-enabled breast pumps into sensitive compartmented information facilities (SCIFs)
• Publication of "Flying While Pregnant" survey
• Childcare resources included in First Term Enlisted Course
• Production of "Childcare Heroes Videos" to promote DoD childcare staff hiring
• Publication of Reserve and Guard guides on parental leave policy expansion
• Updates to DAFI 36-2908, *Family Care Plan*, to clarify policies and requirements
• Child Development Center no hat/no salute guidance added to DAFI 36-2903
• Updated guidance on pregnancy/postpregnancy exemptions for body composition assessment
• Authorized convalescent leave for the nonbirth parent following perinatal loss in DAFI 36-3003, *Military Leave Program*

23. Clayton Filipowicz, "Women's Initiative Team: Taking Initiative, Breaking Barriers," *Airman*, June 7, 2021, https://www.airmanmagazine.af.mil/.

24. Kelly Atkinson and Alea Nadeem, "Warrior Braids and the Air Force Women's Initiative Team – The Invisible Labor behind Diversity, Inclusion, and Institutional Change," Wild Blue Yonder, May 17, 2021, https://www.airuniversity.af.edu/.

25. DAF Women's Initiatives Team record of policy change efforts, current as of April 2024.

Table 1 (*continued*)

- Advocacy and coordination on DoD and service guidance for parental leave parity

2022

- Approval of Air Education and Training Command simulator credit to mitigate temporary medical disqualification (i.e., in cases of pregnancy)
- Shaped guidance for Secretary of Defense memo "Ensuring Access to Reproductive Health Care" and DAF guidance on implementing nonchargeable leave for reproductive health care
- Updated AFI 48-145, *Occupational and Environmental Health*, military codes, and profile forms to protect pregnancy privacy
- Partnership with Military Family Building Coalition to expand reproductive clinical advocacy and fertility management services to service women at no cost to member
- Designed and wrote pre-/postpregnancy experience survey, released by Air Force Survey Office (AFSO)
- Updated policy to allow pregnant service members to attend medical readiness training
- Update to AF Manual (MAN) 36-2032, *Military Recruiting and Accessions*, to remove restrictions on pregnant women applying to Officer Training School
- Identified supply deficiency for maternity uniforms and coordinated uniform redistribution worldwide with Army and Air Force Exchange Service
- Update to DAFI 36-3003 to allow permissive temporary duty (TDY) for fertility treatment travel
- Changed Joint travel regulation allowing breastmilk transport cost reimbursement while TDY
- Supported DAF clarification of policy allowing pregnant aviators to return to flying status
- Initiated redesign and funding of new maternity flight suits
- Updated Space Force officer classification guide to expand candidate talent pool degree requirements to bolster more diverse representation
- Air Force Special Operations Command policy update to authorize Bluetooth-enabled breast pumps into SCIFs

2021

- Updated AFMAN 41-210, *Tricare Operations and Patient Administration*, to standardize convalescent leave for pregnancy loss
- Supported DAF guidance memo clarifying pregnancy termination access
- Updated DAFI 36-2110, *Total Force Assignments*, to clarify postpartum TDY deferment policy
- Updated women's hair standards to improve medical, operational, and inclusivity impacts
- Supported DAF guidance on commander accountability for climate assessments
- Transitioned previous guidance memos for lactation requirements to standalone DAFI 36-3013, *Lactation Rooms and Breast Milk Storage for Nursing Mothers*

2020

- Held inaugural Women's Air and Space Power Symposium 2020

Table 1 (*continued*)

- DAF policy updated to direct that anthropometric design specifications must accommodate body sizes of at least the central 95 percent of the US recruiting population, including all races and genders
- Air Force awarded contract to begin production of female body armor
- Sponsored redesign of maternity service dress by Squadron Officer School students
- Updated Military Equal Opportunity Program DoD Instruction 1350.02 to include pregnancy
- Supported Air Force removal of minimum height requirement for aviation applications
- Initiated Air Force allowance of fitness assessment exemptions for miscarriages
- Partnered with AFWERX to distribute free fertility kits to service women
- Led Air Force removal of administrative policies preventing pregnant and postpartum women from attending PME
- Established Air Force policy mandating nursing mother access to refrigerator in work center
- Changed policy to allow women option to wear pants with mess dress uniform
- Modified existing flight suit uniforms for pregnant women
- Built and launched Kinderspot app to centralize and streamline childcare spot subletting

2019

- Coordinated with base uniform stores for maternity uniforms to be available in person
- Established Air Force-wide creation of civilian voluntary leave bank program in AFI 36-815, *Leave*
- Held inaugural WIT strategic offsite
- Partnered with AFSO to launch first survey on maternity uniform redesign
- Secured authorization for remotely piloted aircrew, missile operations duty crews, and specified fully qualified pilots to perform duties while pregnant, without medical waiver
- Led female fit program event to develop two-piece female flight suit, improve current women's one-piece coverall, and advance aviator bladder relief system for Air Force and Navy
- Initiated guidance memo 2019-36-02 to require organizations to have dedicated lactation rooms
- Facilitated pregnant Airmen to become eligible to log gate months while pregnant

2018

- Partnered with Department of Veterans Affairs to create Women's Health Transition course
- Updated AFI 36-2903 to authorize wear of breastfeeding undershirt in uniform

2017

- Established Air Force national capital region pilot program for civilian voluntary leave bank

Table 1 (*continued*)

2016
• Supported Air Force implementation of new DoD-wide policy providing female active-duty Airmen up to 12 continuous weeks of fully paid maternity leave
• Mandated use of diverse hiring panels for all GS 14/15 positions
• Modified policies relating to civilian developmental education
• Initiated new policy requiring Air Force Personnel Center commander approval when proposing to separate dual military spouses for assignments
• Revised policy allowing pregnant Airmen the option of applying to separate from military service commitment, now extending timeline from pregnancy to first year postpartum
• Initiated option for officers to decline in-residence intermediate or senior development education without seven-day separation or retirement requirements

Theoretical Application: The WIT and Agents of Institutional Change

Considering the purpose and policy change accomplishments of the Women's Initiatives Team, the framework for categorizing agents of institutional change illuminates the mechanisms of WIT policy change efforts. Referencing figure 1 above, the population under consideration includes members of the Air Force and Space Force, including military and civilian personnel. Within the DAF, power most simply derives from rank: the higher the rank, the more organizational and positional power the member possesses within the institution. Interest refers to a member's interest in WIT policy change efforts, broadly defined as gender policy change.

Within this system, the majority of WIT members fall in the category of change agents. These are typically individuals who have moderate levels of rank-based military power coupled with a high interest in gender policy change. But the existence of these change agents cannot be taken as a given; rather, path-dependent analysis reveals the foundation for why this population might exist in the first place.

The Women's Armed Services Integration Act of 1948 institutionalized women's World War II military contributions by allowing them to serve as "regular members of the Army, Navy, Air Force, and Marine Corps."[26] Of course, participation does not equate to power within an institution. Despite the Integration Act becoming law in 1948, women were not admitted to the US Air Force Academy, the nation's largest producer of commissioned officers, until 1976, with the first women graduating in 1980.[27]

This timeline is critical when considering how power operates in the military system, defined elsewhere as a "greedy" societal institution subject to change and depen-

26. C. Todd Lopez, "In 75 Years Since Women's Armed Services Integration Act, Female Service Members Have Excelled," US Department of Defense (DoD), June 12, 2023, https://www.defense.gov/.

27. Terri Moon Cronk, "Women in the Military Academies: 40 Years Later," DoD, October 2, 2020, https://www.defense.gov/.

dent on internal and external factors.[28] For example, legal command authority in the US military resides in the hands of commissioned officers. This is not to say that enlisted personnel lack power, but rather that legal authority and chain-of-command power operate through officer personnel structures. The military officer promotion system is structured so that it takes approximately twenty-five years before an individual is eligible for the rank of general officer.[29]

Even within the category of general officer, an individual must serve additional years before reaching the highest rank and with it the highest level of institutional power. In all, it takes roughly 30 years to produce a four-star general. This means that the first female graduates of the Air Force Academy were not eligible for the highest rank in the service until around 2010. Indeed, the first female four-star general in Air Force history is General Janet Wolfenbarger, who graduated in the first class of female cadets from the Air Force Academy in 1980 and reached the rank of four-star general in 2012.[30]

When considering how institutions change, the "firsts" may serve as symbols of change but may often remain focused on moving through and succeeding in the system rather than changing its rules.[31] Overcoming the collective action problem facing policy change therefore requires a larger population of change agents. Research indicates that companies consisting of over 30 percent women financially outperform those with lower levels of women participants, while gender quotas for women's political participation at a minimum mandated threshold of 30 percent correlate with significant effect outcomes.[32] With women making up only 21.4 percent of Air Force and Space Force members as of 2022, the population of institutional members with potential interest in gender policy change falls below the 30 percent threshold.[33] How, then, has the Women's Initiatives Team achieved its policy change successes?

The individual and group dynamics central to WIT policy change efforts benefit from contingent elements of time and visibility. Made visible through path-dependent analysis, these contingent elements change levels of group membership among the general population, change agents, power brokers, and the frozen middle as categorized in the framework presented above.

---

28. Mady Wechsler Segal, "The Military and the Family as Greedy Institutions," *Armed Forces & Society* 13, no. 1 (1986).

29. "Promotion Timing, Zones, and Opportunity," RAND Project Air Force, accessed March 20, 2024, https://www.rand.org/.

30. "First Air Force Female Four-Star General Confirmed," USAF, March 28, 2012, https://www.af.mil/.

31. Frida Linehagen, "Conforming One's Conduct to Unwritten Rules: Experiences of Female Military Personnel in a Male-Dominated Organization," *Res Militaris* 8, no. 1 (2018).

32. Sundiatu Dixon-Fyle et al., *Diversity Matters Even More: The Case for Holistic Impact* (New York: McKinsey & Company, December 5, 2023), https://internationalwim.org/; and Jennifer Rosen, "Gender Quotas for Women in National Politics: A Comparative Analysis across Development Thresholds," *Social Science Research* 66 (2017).

33. Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy, *2022 Demographics: Profile of the Military Community* (Washington, DC: DoD, 2022), https://www.militaryonesource.mil/.

From the time perspective: throughout the 75 years since women were integrated into the military, more women joined the general population as modeled in figure 1 above. As female leaders secured officer commissions and enlisted leadership roles and subsequently progressed higher in rank, they began filling power broker roles. Most importantly, key power brokers emerged who lacked senior leader positional authority but understood how to navigate the bureaucracy, thus making the invisible work of policy change visible.[34]

From the visibility perspective: as power brokers made WIT gender policy change more visible, members of the general population realized that institutions could change, as evidenced by the aforementioned hair policy change. With this realization, they moved into the change-agent category. As this category grows larger, it becomes easier to overcome the collective action problem—both because more members of the change-agent population (in this case, women in the military) exist and because others gain interest in gender policy change for nonutilitarian reasons, such as caring more about about diversity, equity, and inclusion.[35]

The Continued Problem of the Frozen Middle

Although progress has been made, change agents and power brokers—key senior leaders—face risk when engaging the frozen middle. In the context of the Air Force and Space Force, the frozen middle represents a mix of those ideologically opposed to policy change and those whose low interest levels result from their overtasked and underresourced work constraints. In either case, WIT members often expend political capital in their pursuit of gender policy change.[36] This renders deleterious effects on some change agents' careers, given the up-or-out nature of promotions that impact career advancement in the military.

Continued visibility on the operational impact of gender policy change efforts, whether influencing retention, recruitment, operational effectiveness, or other areas, offers opportunities to reduce the strength of the frozen middle's resistance by increasing their interest in gender policy change. Events like the annual Women's Air and Space Power Symposium, which features ongoing efforts of the WIT and other barrier analysis working groups, showcase the power of visibility in the work of policy change.[37]

Conclusion: Applications to Broader Cases

Overall, examining the individual and group dynamics shaping the gender policy change efforts of the DAF Women's Initiatives Team offers novel insights into an un-

34. Atkinson and Nadeem, "Warrior Braids,"

35. "Gen Z Demands Diversity and Inclusion in the Workplace," World Economic Forum, accessed March 20, 2024, https://www.weforum.org/.

36. Atkinson and Nadeem, "Warrior Braids."

37. SecAF PA, "DAF Hosts 3rd Virtual Women's Air and Space Power Symposium," USAF, February 27, 2023, https://www.af.mil/.

derstudied aspect of institutional change—the people involved in the effort. Employing a case study of the WIT shows how a framework for agents of institutional change augments the traditional rational actor framework with historical context and analysis of contingent events. Incorporating the critical role of power adds important context to this area of study.

Future research should explore empirical outcomes of WIT policy change efforts and more details on the group dynamics of the team as a change-agent organization. For example, the internal identity dynamics within the WIT merit exploration, as its members may have different experiences regarding their ability to effect change and their recognition for these change efforts, both internal to the Women's Initiatives Team and from an external audience. This information would prove insightful to ongoing efforts to effect policy change, both in terms of diversity, equity, and inclusion and more broadly.

Moreover, highlighting the different groups that operate along axes of power and interest reveals mechanisms to advance inclusive policy change efforts: when groups understand the motivations behind the frozen middle's resistance to institutional change, they can leverage new approaches to engage this population.

As economic globalization, rapidly evolving technology, and the erosion of international norms continue to transform the global world order, the role of institutions in this evolution proves worthy of particular attention. Understanding the factors that shape agent behavior and how agents themselves transform institutions is critical to understanding, explaining, and predicting political and sociological events in the years ahead. Individuals' motivations and their ability to access power are essential elements to the study of institutional change. Without addressing these areas of study, we will never know the complete picture behind why policy change efforts take flight. Æ

Mission Statement

Æther: A Journal of Strategic Airpower & Spacepower (Æther) is the flagship strategic journal of the Department of the Air Force, fostering intellectual enrichment for national and international security professionals. *Æther* provides a forum for critically examining, informing, and debating national and international security matters as they relate to airpower and spacepower. Contributions to *Æther* will explore issues relevant to national and international security as they relate to national and international airpower and spacepower.

Disclaimer

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

Comments

Please email your comments, suggestions, or address change to **aether-journal@au.af.edu**

Article Submission

Æther: *A Journal of Strategic Airpower & Spacepower* considers scholarly articles between 4,000 and 6,500 words from US and international authors. Please send your submission in Microsoft Word format via email to **aether-journal@au.af.edu**

Æther: A Journal of Strategic Airpower & Spacepower
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112–6026

View and subscribe for free to *Æther* at
https://www.airuniversity.af.edu/AetherJournal/

Follow *Æther* on Facebook, LinkedIn, X, and Instagram.

Æther (ISSN 2771-6120) is published by Air University Press, Maxwell AFB, AL.

Æther is indexed in, inter alia, Proquest, Gale-Cengage, Ebsco, JSTOR, and DTIC.

A FORUM FOR CRITICALLY EXAMINING, INFORMING, AND DEBATING NATIONAL AND INTERNATIONAL SECURITY MATTERS AS THEY RELATE TO AIRPOWER AND SPACEPOWER

HTTPS://WWW.AIRUNIVERSITY.AF.EDU/AETHERJOURNAL