SSQ
STRATEGIC STUDIES QUARTERLY
SPRING 2021 VOL. 15, NO. 1

SSQ Strategic Studies Quarterly

https://www.af.mil/

https://www.spaceforce.mil/

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

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

Strategic Studies Quarterly

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

SPRING 2021 VOL. 15, NO. 1

POLICY FORUM

FEATURE ARTICLE

PERSPECTIVES

BOOK REVIEWS

The Missile Defense "Arms Race" Myth

US policy toward ballistic missile defense (BMD) of the homeland is designed to stay ahead of the rogue state threat while relying on nuclear deterrence to prevent an attack from the nuclear missile arsenals of Russia or China. Today, the United States has 44 ground-based interceptors (GBI) and plans to increase the total number of its most capable interceptors to 64 by 2030 with the deployment of the Next Generation Interceptor. After its recent successful test against an intercontinental ballistic missile (ICBM)-type threat, the United States is also examining how the Standard Missile-3 (SM-3) Block IIA could complement GBIs in a layered homeland missile defense architecture.

Domestic critics of US homeland missile defense, as well as Russia and China, claim that increased US missile defense capacity and capability will lead to an arms race. They assert that it will stimulate Russia and China to build more offensive missiles in response, ultimately making the United States less safe. The critics' logic also assumes that US restraint in missile defense will obviate Russian and Chinese perceived needs for missile modernization and production. These individuals predict a prototypical action-reaction dynamic that has little empirical support and deserves great scrutiny.

Russian Reaction to US Missile Defenses

Broadly speaking, Russia could react in two ways to overcome perceived advances in US missile defense: proportionally or disproportionately increase the overall number of missiles, launchers, and reentry vehicles in an attempt to overwhelm US missile defense capacity, or develop specific weapon systems meant to evade US missile defenses. Evidence for the first reaction is severely lacking while evidence for the second is mixed at best.

Beginning in 2000, when it became a serious possibility that the United States might pull out of the Anti-Ballistic Missile (ABM) Treaty that limited missile defenses, one would expect Russia to react—according to the "arms race" logic—by increasing the numbers of its missiles, launchers, and reentry vehicles. However, the number of Russian ICBMs and submarine-

*The online version of this article has additional references hyperlinked in the text.

launched ballistic missiles (SLBM)—the systems most likely to be adjusted to counter advances in US missile defenses—and their associated launchers and reentry vehicles declined substantially. Open source, estimated numbers tell the story. In 2000, analysts believed that Russia had 756 ICBMs and 348 SLBMs, totaling 1,104. Five years later, analysts believed that Russia had 585 ICBMs (down 23 percent) and 192 SLBMs (down 45 percent), totaling 777 (down 30 percent). In 2010, analysts believed that the number of ICBMs fell 43 percent and SLBMs 17 percent, a combined reduction of 37 percent. Russian ICBMs and SLBMs have remained at 2010 levels, with minor variation, through today. There is no perceptible arms race here.

Perhaps Russia placed more warheads on its missiles to overcome US missile defenses? Again, the data do not support such a mechanical action-reaction. Russia in 2000 had an estimated 5,116 warheads dispersed between ICBMs and SLBMs. In 2005, that estimate was 2,942, down 42 percent. In 2010 and 2015, estimates were at 1,666 and 1,721, respectively. Today, Russia is estimated to have 1,856 warheads. These numbers indicate a small increase in the past 10 years, yes, but it is hardly attributable to US missile defense—much less shows evidence of an arms race. More likely, the increase can be attributed to Russia's ongoing nuclear modernization that is replacing older systems with newer systems.

Some may counter that Russia could not respond to US missile defense increases because of strategic arms control treaties with the United States. Indeed, Russian forces were constrained by such treaties, but Russia would likely never have agreed to those force limits unless it felt secure enough in its force composition to do so. Certainly, it was aware of the potential for US homeland missile defense improvements.

Furthermore, as Lt Gen Robert Ashley, US Army, retired, stated in 2019 when serving as the Defense Intelligence Agency director, the United States expects the Russian nuclear arsenal to grow "significantly" over the next decade. However, that growth "is primarily driven by a significant projected increase in the number of Russia's non-strategic nuclear weapons" (i.e., short-range weapons, not the long-range weapons one would expect if there was an overriding impetus to compete in an arms race to offset US homeland missile defense advances).[1]

Likewise, Cold War data do not support the inverse of the critic's argument: that the US refraining from building missile defense lessens the need for Russia to build more missiles. From 1972 to 1982, a time when the United States built and then completely dismantled its only limited homeland missile defense system, the Soviet Union increased its number

of ICBM reentry vehicles from about 1,500 to almost 6,000 total. SLBM reentry vehicles, in the same period, increased from 500 to about 1,500.[2] Again, US restraint in building missile defenses apparently did nothing to discourage a Soviet buildup in offensive missile forces.

If building additional or more capable US missile defenses will not necessarily lead to an increase in Russia's missiles or reentry vehicles, what then can be said for the second argument? Will building more US missile defenses stimulate an asymmetric Russian reaction to build weapon systems specifically designed to negate or evade US missile defenses, thus making the US less safe? On this point, critics may find firmer ground, but the evidence is mixed at best.

It is undeniable that Russian president Vladimir Putin's attitude toward US missile defense plans has consistently ranged from skeptical to outright hostile; he has regularly declared that Russia will take the necessary steps to respond, specifically with its own asymmetric weapons programs. To cite just one of many examples, President Putin stated, "I want to say that the United States, when it withdrew from the ABM Treaty in 2002, forced us to begin developing new weapon systems. We told our partners about it, and they said, 'Do whatever you like.' Fine, that is what we did—so enjoy."[3] And, indeed, as detailed in President Putin's speeches to the Federal Assembly, he has ordered a number of new exotic systems be built in response to US homeland missile defenses.

But does this settle the matter? If the US had remained in the ABM Treaty, would Russia not have built these systems, and would the United States be safer? We must examine these new Russian "super weapons" as evidence of Russia's response.

The first is the SS-X-29, a super-heavy ICBM, reportedly capable of carrying 10 reentry vehicles and nicknamed in the West as the "Son of Satan." "Satan" was the NATO designator of the missile that Russia will likely replace—the SS-18, which can also reportedly carry 10 reentry vehicles. The SS-18 itself was a replacement for the SS-9 Scarp, and its primary missions were reportedly destroying US ICBM fields and penetrating possible US missile defenses. But the SS-18 was originally deployed in 1975 and continued being fielded throughout the '70s and early '80s when the United States had zero missile defenses.[4] In the context of nuclear arms control, it might be advantageous to have the capability of loading a relatively large number of warheads on a single missile when the number of missiles is limited. It is likely then that Russia views having this new super-heavy ICBM as much more than just a missile defense killer, and it was certainly not built solely as a response to US missile defenses.

The second and third new weapon systems that Putin claims are in response to US missile defenses are the SS-19 Mod-X-4 (Avangard) hypersonic glide vehicle (HGV) and the Kinzhal air-launched ballistic missile. While the Kinzhal seems more likely to be used in a geographically limited conflict rather than for penetrating US homeland missile defenses, the Avangard HGV appears at first glance to be a direct counter to US missile defense. It seems designed to outmaneuver any BMD interceptor. But Russian officials plausibly may have wanted an HGV even if the United States had no missile defenses. Due to their low flight altitude, HGVs can literally "fly under the radar" of terrestrial-based radars pointed into space. This makes the HGV detectable much later in flight, giving the United States less strategic warning. Indeed, Russian officials could view Avangard as useful for targeting US radars, BMD sites, or time-sensitive assets. Again, Russia would likely find Avangard to be advantageous even if there were no US homeland missile defenses.

Finally, the fourth and fifth of Putin's nuclear "super weapons" have the most plausible argument in being direct responses to US missile defenses. The "Poseidon," a nuclear-powered "transoceanic nuclear[-armed] torpedo," will evade US missile defenses by operating underwater. In addition, Russia is developing the "Burevestnik" nuclear-powered, nuclear-armed cruise missile, which Putin specifically mentions having "unlimited range" and is useful for avoiding missile defense. These two systems do seem to validate critics' claims that without the US building up its missile defenses, these Russian systems would have no purpose and would not have been built, thus increasing US security.

Even this apparent action-reaction dynamic, however, is not proof enough of US missile defenses' allegedly destabilizing nature. As Rose Gottemoeller, former NATO deputy secretary general, recently stated, it is not obvious that Russia views these nuclear-powered novelties as having real operational value for bypassing US missile defenses. She notes,

> These exotic systems have more of a political function than a strategic or security one. Their role is to signal Russia's continuing scientific and military prowess at a time when the country does not otherwise have much on offer. Devilishly expensive and sometimes dangerous to operate, they are unlikely to be deployed in big numbers, as a 2019 fatal testing accident of the Burevestnik shows. . . . The exotics don't add to that [strategic] deterrent. They have some show-off value, but they will do no more than make the rubble bounce.[5]

If these systems do come to fruition, they will be inherently redundant for a mission that Russia can already accomplish: penetrating and over-

whelming US missile defenses. The United States designed and built its homeland missile defenses to defeat only rogue state ICBMs—not the much more advanced Russian or Chinese missiles that can accommodate missile defense countermeasures. Thus, Russia gains practically no security advantage in developing these exotic nuclear weapons. In fact, US homeland BMD may have unintentionally imposed costs on the Russian defense sector—causing Russia to invest untold millions of rubles into redundant systems. Every ruble it invests in these exotic systems is not invested in systems that could threaten a perceived US weakness.

More importantly, US homeland defense efforts lose none of their effectiveness or value if Russia may more easily defeat them. The purpose of US homeland missile defense is to defend against rogue states, not Russia or China. While Russia's reactions to US missile defense show little evidence of an arms race dynamic, China's reaction may provide additional insight into this debate.

Chinese Reaction to US Missile Defenses

Just as with Russia, there are two broad ways of potentially demonstrating that the buildup of US missile defenses would likely cause a buildup of China's intercontinental-range missiles. First, one can examine the number of China's intercontinental-range missiles and associated reentry vehicles over time, especially the period from 2000 to today. Indeed, in the past 20 years there has been a substantial increase in the number of Chinese intercontinental-range systems and their associated warheads. In 2000, according to open sources, China had about 20 ICBMs and associated warheads. By 2010, those numbers had risen to approximately 40, and by 2020, China possessed approximately 98 ICBMs with 138 associated warheads and 48 (intercontinental-range) SLBMs and associated warheads—all of which could conceivably reach the United States and overcome US homeland missile defenses. These increases do indeed line up with the steady US improvement in the capability and quantity of missile defense interceptors over the same period.

But does this apparent correlation equal causation? During this same time, the United States also increased its conventional capabilities and signaled a much greater focus on defending its interests in the Pacific. In addition, the United States is just beginning to modernize its entire nuclear arsenal, from missiles to submarines to bombers. Meanwhile, Russia has modernized its nuclear forces on its border with China. Any of these factors could be the basis for China's growing intercontinental-range missile arsenal, without mentioning some intangible factors such as wanting

to demonstrate its scientific prowess as a great power. Finally, two years before President Bush decided to withdraw from the ABM Treaty in 2001 and pursue homeland missile defense, the US intelligence community was already projecting a relatively significant growth in the Chinese intercontinental-range nuclear arsenal—indicating that China may have at least partially planned the growth of its missile forces without US missile defense in mind. It is difficult to describe the slow and steady buildup of Chinese intercontinental-range missiles as an arms "race" (the next 20 years might be a different story), much less solely attributable to US homeland missile defense enhancements.

If the overall size of the Chinese intercontinental-range nuclear force cannot provide definitive proof of an action-reaction dynamic with US missile defenses, perhaps its composition—the types of weapons China is producing—can provide clues. China has, and is developing, missiles capable of delivering multiple reentry vehicles. Whether China views this capability as mainly aimed at defeating US missile defenses or simply being able to threaten multiple targets with one missile, or both, is impossible to say with certainty. China is also developing hypersonic glide vehicles, seemingly designed to defeat US missile defenses. But, as explained with Russian HGVs, China may value the element of reduced attack warning provided by its HGVs just as much as their counter-missile defense capabilities. In any case, it is certainly not clear that if the United States refrained from improving its homeland missile defenses, China would have acted any differently in building new systems. Again, just as with Russia, China is likely increasing its forces in proportion to its national strategic aims, regional ambitions, and threat perceptions—of which US missile defense is only one factor, and likely a minor one, among many.

Conclusion

The available open-source data, culled from the Cold War to the present day, on the numbers and types of Russian and Chinese intercontinental-range systems and their associated warheads does not indicate a direct, discernable, or predictable relationship between the size and capability of US missile defenses and Russian and Chinese missile developments. While it appears that Russia and China believe they have reacted to US missile defense developments, it is far from clear how those unique reactions are manifest in their numbers or types of weapons, and there is good reason to suspect they might have done the same things even in the absence of US missile defenses. In short, Russian and Chinese reactions to US homeland

missile defense in the past cannot reasonably be called an "arms race," and present trends in the arsenal can be attributable to range of factors.

While perhaps counterintuitive, the point should not be surprising. When the US government asked similar questions about the action-reaction dynamic between the nuclear arsenals of the US and USSR during the Cold War, some of the brightest minds, given access to the full collection of intelligence, came to a similar conclusion. The consensus was that "the facts will not support the proposition that either the Soviet Union or the United States developed strategic forces only in direct immediate reaction to each other." Or paraphrasing then-US secretary of defense Harold Brown, "When we build, they build; when we cut, they build."

The motivations behind the decisions of what type of missile to build and how many are so numerous and variable that they defy direct, mechanical-like linkage and formulation. We must advance the field of study by eschewing simplistic and unsupported "arms race" rhetoric and focus instead on the unique cultural, historical, and bureaucratic factors that influence threat perceptions, technological innovation, and weapons procurement. Anything less will provide an incomplete threat picture and cause avoidable misperceptions—an unacceptable outcome for a subject where the consequences of being wrong are by nature strategic. SSQ

Matthew R. Costlow
Senior Analyst, National Institute for Public Policy
Former Special Assistant for Nuclear and Missile Defense Policy, Department of Defense

Notes

1. Lt Gen Robert P. Ashley, Jr., "Russian and Chinese Nuclear Modernization Trends" (remarks, Hudson Institute, Washington, D.C., 29 May 2019), https://www.dia.mil/.
2. US Department of Defense, *Soviet Military Power*, 2d ed. (Washington, D.C.: Government Printing Office, 1983), 19, 23, http://insidethecoldwar.org/.
3. Vladimir Putin, quoted in "Interview to American TV Channel NBC," President of Russia website, 10 March 2018, http://en.kremlin.ru/.
4. Pavel Podvig, ed., *Russian Strategic Nuclear Forces* (Cambridge, MA: The MIT Press, 2001), 215–17.
5. Rose Gottemoeller, "Russia Is Updating Their Nuclear Weapons: What Does That Mean for the Rest of Us?," Carnegie Endowment for International Peace, 29 January 2020, https://carnegieendowment.org/.

FEATURE ARTICLE

Codifying *Jus in Bello Spatialis*—The Space Law of Tomorrow

Fabio van Loon

Abstract

From the 1950s to the modern day, the race for space has embodied the classical geopolitics of great power competition.[1] As early as 1961, 80 percent of the astronautic community's members agreed "that there are strategic areas in space which may someday be as important to space transportation as the Panama Canal is to ocean transportation."[2] Today, this geopolitical reality is defined by the acceleration of highly militarized space programs and a competition for outer space's strategic areas in tomorrow's ultimate high ground. In preparing for the war-fighting domain of the future, the US can and must lead in defining *jus in bello spatialis*—the law of armed conflict in space. This article assesses the current framework of international space law and recommends ways the United States can lead in enhancing today's space security and in creating tomorrow's rules of the road. The proposed approach would strengthen existing protections for astronauts and satellites in the context of military escalation, conflict, and resolution.

*****

With a deep-rooted history of customary space law, state activities in outer space have largely been established for the areas of research, exploration, and scientific inquiry.[3] The teleological origins of today's space law—namely the principles of peaceful exploration and the freedom of navigation—were candidly expressed by President Dwight D. Eisenhower in a letter he wrote to then-Soviet premier Nikolai Bulganin in 1958. He stated, "I propose that we agree that outer space should be used only for peaceful purposes. We face a decisive moment in history in relation to this matter. . . . Should not outer space be dedicated to the peaceful uses of mankind and denied to the purposes of war?"[4]

President Eisenhower's commitment to cosmic peace in the opening months of the space race proved foundational to the negotiation of the historic Outer Space Treaty (OST) a decade later, the keystone of today's *corpus juris spatialis*—the body of law in space. The 1967 Outer Space

Treaty, similar to the landmark 1963 Limited Test Ban Treaty (LTBT) and 1972 Anti-Ballistic Missile (ABM) Treaty, epitomized the success of international legal cooperation. Mutual restraint, advanced through the treaty's notion of space as "the province of all mankind," effectively prevented the likely weaponization of space both during and after the Cold War.[5] Washington's leadership in defining and upholding the principles of international space law has since guaranteed peace in the cosmos for over 60 years, a testament to the successes of American space diplomacy and the strength of international space law.

Today, evolving security challenges in the outer space environment have placed an unprecedented strain on the stability of the international space regime. The challenges of the return to great power competition in space have been compounded by the seemingly unavoidable militarization of the cosmos. This issue has highlighted how the "customary principles of this body of law are probably neither sufficiently specific nor entirely appropriate for military action in outer space."[6] Filling this normative void in the spirit of national and international security must be at the center of US-led efforts to draft and define tomorrow's *jus in bello spatialis*. Ultimately, to determine tomorrow's law of war in space, strategists must pay particular attention to the normative applicability of the UN Charter, the compelling analogy of the high seas, the law of armed conflict (LOAC), and existing protections for astronauts and satellites.

The Applicability of the UN Charter

Today, the UN Charter's applicability to space affairs is hardly disputed. Historical precedent includes Dutch international legal scholar Daniel Goedhuis's statement in 1967 that "international law is '*ipso jure*' [by the law itself] applicable extra-terrestrially." Further, he asserts that "the relevant rules of international law must be taken to regulate international relations wherever such relations take place."[7]

Evolving from historic precedent, today's international consensus stems from the customary law established by both Soviet and US leadership in the 1960s. In "Soviet Legal Views on Military Space Activities," lecturer Malcolm Russell states that "East and West both share the view that States have the same right to exercise self-defense in space that they do on earth."[8] This view was clearly expressed in the 2001 *Report to the Commission to Assess United States National Security Space Management and Organization*, which specifies that "a number of existing principles of international law apply to space activity. Chief among these are the definition of . . . the right of self-defense."[9]

The US government's most explicit support for self-defense in space as provided for in Article 51 of the UN Charter was voiced in 2002 by then-US ambassador to the Conference on Disarmament (CD) in Geneva. He argued, "Article 51 of the UN Charter makes it clear that all Member States have the inherent right of individual and collective self-defense. The global responsibilities of the United States, and the new threats facing it in today's world, require that that right be exercised both on the Earth and above it."[10]

While the 1967 Outer Space Treaty has forbidden the stationing of nuclear arms and other weapons of mass destruction (WMD) in space, Bruce Hurwitz argues that the treaty has "not prohibited the use of outer space *sensu strictu* [in a strict sense] for all military purposes."[11] In fact, by invoking the direct applicability of the UN Charter, the OST indirectly provides support for the use of force through the concept of state sovereignty. Article VIII of the treaty specifies that the state launching a space object retains jurisdiction over it regardless of its location, so "if jurisdiction is equivalent to sovereignty," then "the right of a State to defend objects under its sovereignty on earth logically extends to outer space."[12] Implying the sovereignty over its own installations, it seems reasonable that a state "may take appropriate steps for self-protection."[13] Following this logic, the foundational document of modern space law clearly affords states "the right to defend themselves in, from and through outer space."[14]

Through the explicit application of the UN Charter as generally accepted law (*lex generalis*) to outer space, the customary legal practice of states led Goedhuis to contend that the majority of states have accepted that, in accordance with the 1967 Outer Space Treaty, some "military activities are legal."[15] In this regard, international law professors Jackson Maogoto and Steven Freeland indicate that "the legal regime that governs the possible weaponization of outer space is . . . largely protective of a State's sovereign right to utilize force in self-defense."[16] Through the development of Earth- and orbit-based antisatellite technologies, this view has been accurately reinforced via the practice of spacefaring states, thereby cementing the norms of the Outer Space Treaty and the UN Charter into customary international space law.[17]

Readers must therefore note that the OST, routinely "referred to as the Magna Carta or constitution of outer space," has consistently shaped and refined state practice from its inception.[18] By the same token, it could also be argued that the OST was developed in parallel to the emerging customary law of the 1960s. This observation is validated by the content of the OST's provisions, largely reflecting that of the 1959 Antarctic Treaty—

particularly regarding the exploration and non-appropriation of territory. Similarly to the Antarctic Treaty, the OST reflects an international desire to prevent "a new form of colonial competition" in space, confirming the spirit originally expressed by President Eisenhower in 1958 that space must remain an environment "denied to the purposes of war."[19]

The Law of Space and the High Seas Analogy

Arms control theorists have conceived of several legal analogies to drive the debate on creating a more "elaborated normative regime" in space.[20] This goal was consolidated in paragraph 4 of the OST preamble, which states the desire "to contribute to broad international co-operation in the scientific as well as the legal aspects of the exploration and use of outer space for peaceful purposes."[21] In an effort to respond to the threats of weaponization while operating within the realm of realistic arms control, legal experts have theorized and proposed the application of a variety of arms control analogies, the most practicable of which is the analogy to the high seas.

Today, the high-seas analogy—based on the Roman law tradition of *res communis* (the common heritage of mankind)—is a core tenet of US space strategy. Historically evolving from the successful high-seas legal regime, international space law is primarily based on the freedom of navigation and exploration. In drafting and negotiating the foundations of modern space law to incorporate the core spirit of free, unrestrained exploration, Everett Dolman notes that "the United States desperately wanted to have the prevailing notion of innocent passage as reflected in the law of the sea applied to outer space." Further, the US did not want "to allow an upward extension of existing air law, in which territorial ownership extends upward, *usque ad coelum* (as far as the sky)."[22] In fact, according to Hurwitz, "the exercise of self-defense in outer space may be viewed as analogous to its exercise on the high seas, or in any other areas where a State is taking action outside of its territory."[23] While this view may find support in elements of the US national security establishment, it has not yet been established as customary law in the space environment.

Modern advocates of arms deployment in space have regularly relied on this rationale, specifically the freedom of the seas as an environment where naval power may be boundlessly projected under customary international sea law. University of Exeter professor Kubo Mačàk contends that "this longstanding interpretation . . . has been reflected in the widely respected 1994 *San Remo Manual*, according to which hostile actions by naval forces may be conducted in, on, or over . . . the high seas."[24] In this view, similarly

to the high seas, the UN Charter is interpreted as not providing restrictions on state activity while simultaneously providing protection for states against aggression under Article 51. The analogy to instruments of maritime law, such as the 1994 *San Remo Manual*, seeks to ensure the "peaceful purposes" of space while guaranteeing the traditional conventions of freedom of exploration and lawful military activities. Just as the authors of maritime law envisioned "peaceful purposes" for military operations, they guaranteed more or less "unrestricted military activities in the high seas."[25] This invariably affected the modern form of *jus ad bellum* as to how and when navies could rightfully engage an adversary—simultaneously ushering in a distinct form of *jus in bello*. While this legal framework has proven to be a successful guarantor of peace in space for over 60 years, the waning security of the global commons leaves the largely unprotected US satellite systems "on the open seas of space" in a position of profound vulnerability.[26]

The Applicability of the Law of Armed Conflict

According to the *Routledge Handbook of Space Law*, "When the use of force in space occurs, the *jus in bello*, currently called the law of armed conflict (LOAC) or international humanitarian law (IHL) applies."[27] However, lacking codified legal mechanisms for the conduct of hostilities in the event of an armed conflict, the law of cosmic war remains largely to be determined.[28] Despite this normative impasse, two international nongovernmental diplomatic initiatives, similar in nature to the 1994 *San Remo Manual*, are currently endeavoring to restate, define, and provide guidelines for the interpretation and application of international legal instruments to military operations in space. The *Woomera Manual* and the *Manual on International Law Applicable to Military Activities in Space* (MILAMOS) are leading international efforts to develop the rules of the road for an increasingly competitive space environment. In articulating and further defining the law that applies to military activities, these projects respond to the normative void of today's *jus in bello spatialis* by contributing, as the MILAMOS website affirms, "to a future where all space activities are conducted in accordance with the international rules-based global order."[29] Considering how space law has lagged the development of military space capabilities, these efforts are of crucial importance.[30]

Nonetheless, considering the current potential for the militarization of national space assets (both satellites and other astronautic operations), LOAC provisions remain highly relevant in the conduct of space activities. Given the extent of lethality ensured by space-based directed-energy weapons, kinetic weaponry (missiles), electromagnetic pulse (EMP), or

potentially nuclear armaments, it is imperative that legislators, diplomats, and national space agencies work toward the drafting of key *jus cogens* prerogatives. *Jus cogens,* or peremptory norms also known as matters of "compelling law," are norms from which no derogation is permitted. These norms—typically addressing war crimes, acts of genocide, and other crimes against humanity—"reflect and protect fundamental values of the international community, are hierarchically superior to other rules of international law and are universally applicable."[31]

In this regard, the most encompassing instruments of international humanitarian law—the Geneva Conventions—are highly applicable to space and are a valuable point of departure for the drafting of said *jus cogens* provisions. While terrestrial operations are hardly comparable to those carried out in space (and will remain so for the foreseeable future), the issue of war in space—and perhaps that of one entirely waged in space, however unrealistic it may seem—must be contended with.

Mačàk argues that applying customary (terrestrial) *jus in bello* law to outer space would "alleviate the problem of limited applicability of some of the relevant treaty law."[32] Lacking any specific references to the laws of war in space treaty law, this seems a most appropriate point of departure. Being "well established . . . that the Hague Regulations have acquired the force of customary international law," reinforcing that the principles of customary law would help create a clearer set of conduct for peacekeeping operations, belligerents, and space diplomacy at large.[33]

Unlike conventional terrestrial conflict, conflict in space would rely on capital-intensive technology and a highly specialized cadre of astronautic military personnel. Therefore, it is imperative that the law of war in space develops into a highly specialized, normative regime. To this end, its drafters will likely find the normative framework of the UN Charter, the LOAC, and Geneva Conventions to be a helpful point of departure. That said, the law of space war necessitates a *lex specialis* regime, one prepared to deal with the challenges of an unprecedentedly militarized, twenty-first-century space race. The need for an updated, highly specialized legal framework is heightened by the threats of rapidly advancing ASAT technologies. Modern international initiatives such as MILAMOS and *Woomera* are valuable tools in refining the provisions of the powerful 1967 Outer Space Treaty and are a much-needed springboard for the drafting of tomorrow's law of space.

Reinforcing the Outer Space Treaty's ban on WMDs must remain a key element in informing today's debate on the use of weapons in outer space. The bold and prescient provisions of the OST must be strengthened

and updated to best address present and future challenges. Moreover, it is important to reiterate that "updating" these arms control provisions should not be interpreted as prejudicing or limiting the use of other weapons for self-defense based on terrestrial law and tradition. In fact, maintaining the right to self-defense, while strengthening and refining the OST's ban of WMDs, is the most effective way to address the menace of nuclear weapons in space. Efforts to reaffirm and update the OST are urgent when accounting for the devastating scope of a nuclear weapon detonated from space. According to NASA research, a space denotation could have 8 to 17 times the blast radius of a nuclear detonation on Earth.[34]

Protections for Astronauts

Historically considered the envoys of mankind, astronauts cannot logically be considered combatants—just as military chaplains and paramedics are not in the conventional military. Maj Robert Ramey, USAF, contends that "it would simply be incongruous for one person to simultaneously constitute a combatant and an 'envoy of mankind.' "[35] As noncombatants, states are "prompted by sentiments of humanity" to assist astronauts wherever possible, similarly to individuals in distress on the high seas.[36]

While envoys of mankind are reasonably distinguished from combatants, the distinction may become blurred in a state of war, "as there will undoubtedly be some role for military astronauts in space combat."[37] Whereas astronauts have never been considered military personnel under the auspices of peaceful military exploration, current military developments require an analysis of the relevant, applicable *jus in bello* to their activities in space. In the event of hostilities, would astronauts constitute legitimate military targets? According to Mačák, "Astronauts maintain their status as 'envoys of mankind' and the concomitant rights unless and until they engage in conduct with a material nexus to an armed conflict."[38] Their conduct as combatants would *eo ipso* (by their own account) transform them into legitimate military targets.[39] After all, "there is no reason the term combatant could not apply to military personnel in space just as it does to individuals on land, sea, and air if authorized to engage in armed conflict."[40]

To establish the combatant status of astronauts according to the standards of the 1907 Hague Convention, astronauts must (1) "be commanded by a person responsible for his subordinates"; (2) "have a fixed distinctive emblem recognizable at a distance"; (3) "carry arms openly"; and (4) "conduct their operations in accordance with the laws and customs of war."[41]

In Ramey's view, the classification of astronauts as envoys of mankind is to be interpreted with the object and purpose of the document in which

this view is expressed, namely the OST. The view presupposing the "peaceful purposes" of space activities would be nullified insomuch as belligerent space activities would violate the treaty. In this regard, *jus in bello* norms are certifiably applicable to astronauts who engage in nonpeaceful activities with the astronauts and/or the space assets of other states.

Therefore, in having identified the hostile acts of astronauts in a state of war, UN Resolution 2345 (XXII)—the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (herein termed the Astronaut Convention)—would be null. As stated by Canadian space legal counsel Michel Bourbonnière, "The Rescue Agreement never specifically enounces conditions of war or of use of military force. Furthermore, there is no specific mention of any intent to modify the Geneva Conventions which regulate capture."[42] In this case, *jus in bello spatialis* would, like terrestrial combat, designate captured astronauts as prisoners of war. Though protected under the international humanitarian law of the Geneva Convention, they would not enjoy diplomatic immunity. This caveat would nullify the requirement of the capturing state to return captured astronauts to their launching state as required by the Astronaut Convention.[43] While the Astronaut Convention would cease to enjoy legal value during armed conflict, the Convention "cannot preclude a military astronaut from seeking political asylum since this is a well-established right in international public law."[44] Furthermore, as in the case of a pilot having to evacuate his aircraft, future space law should provide the same protection to Airmen as stated in Article 39(1) of the 1977 Additional Protocol I to the Geneva Convention (AP I), guaranteeing that a military astronaut is not a legitimate target when piloting a disabled spacecraft toward earth.[45]

Protections for Satellites, Neutrality, and Dual-Use Technology

In a state of war, a similar albeit different approach would apply to satellites, which would no longer enjoy immunity as they have historically been accorded by the Conference on Disarmament and Article VIII of the OST.[46] Similarly to astronauts, upon the opening of hostilities, satellites engaging in or facilitating military activities constitute legitimate military targets.[47] While satellites do assume military significance in a state of war, Article 1 of the 1977 Additional Protocol I (AP I) to the Geneva Convention underwrites the need for an attack to minimize all collateral damage.[48] Considering the extent of debris caused by the use of kinetic or directed-energy weaponry, potentially damaging the function-

ality of satellites belonging to third parties or those serving civilian purposes, it has been argued that states should endeavor for a soft kill, reducing collateral damage by using cyber or electromagnetic jamming technology.[49] Following from this concern, "ASAT attacks producing significant amounts of space debris that may affect the orbital environment for decades could be classified as a prohibited method or means of armed conflict under Art. 35 (3) of AP I, depending on the definition of the 'natural environment.'"[50] In addition to violating AP I, creating excessive debris would likely "violate the obligation of due regard for the interests of other States required in the OST (Art. IX)."[51] The use of a highly destructive ASAT weapon, particularly a nuclear weapon, would also violate the Environmental Modification (ENMOD) Convention, which prohibits "any technique for changing—through the deliberate manipulation of natural processes—the dynamics, composition or structure of the earth, of its atmosphere . . . or of outer space."[52]

Naturally, it is also in the strategic interest of the belligerent parties to reduce debris to a minimum—to decrease the chances for collision—while increasing the functionality and orbit of satellites. In conclusion, Art. 36 of AP I stipulates that states that develop and eventually adopt a new weapon are "under the obligation to determine whether its employment would be prohibited by international law."[53] The employment of weaponry creating excess debris would be a clear example of such a violation.

Civilian satellites are protected under Article 52(2) of AP I, expressly ruling out the possibility of "attacks and reprisals against civil objects."[54] Such civilian space assets may be identified through the Registry of Space Objects, stipulated by the 1974 Registration Convention. Civilian satellites may, however, be attacked if the civilian assets are "being used to support military activity."[55]

With a projected threefold increase in the number of both military and (predominately) civilian satellites launched over the next seven years, dual-use satellites concealing offensive capabilities are of ever greater concern.[56] The possibility of satellite jamming satellites that can evade international law and verification has become a key security issue. Civilian satellites can also be equipped with this technology—categorized as a space-stalker threat with dual-use, potentially offensive capabilities.[57] Such technologies include robotic arms and radio frequency jammers and lasers that, while traditionally serving as satellite maintenance and/or communications equipment, may host a range of offensive military capabilities.[58] Under current legal norms, seemingly peaceful capabilities, while in effect offensive in their purpose, could be easily concealed from national

and international compliance monitoring efforts. Assuming the general immunity of civilian assets under customary law, the current state of ASAT legislation, and the Conference on Disarmament's ambitious concept of an international inspectorate, satellite verification may remain difficult if not impossible to effectively implement.[59]

Like the protections for astronauts in peacetime or those serving a nonbelligerent or neutral state, satellites owned by a private firm or a neutral state are generally protected by immunity. However, the Hague Convention affirms that neutral states are not required to "forbid or restrict the use on behalf of the belligerents" of technology used for typically civilian purposes, such as weather or civilian communications satellites.[60] While this protection is generally valid for the satellites of neutral states, neutrality protections could be reasonably voided upon discovery that the neutral state supplied a belligerent with sensitive information or high-tech capabilities such as remote sensing satellite imagery.[61]

The rules of engagement are still to be determined, but attacking satellites would likely be a far more common mode of conflict than targeting astronauts. ASAT weapons include in-orbit threats (i.e., other satellites), direct-ascent land-based ICBMs, or electronic jamming from ground-based transmitters. See figures 1–3 below for a visual representation of direct-ascent attacks, electronic jamming, and a variety of orbital threats.

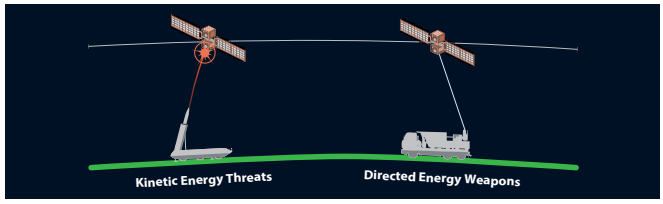

Figure 1. Kinetic and directed-energy weapons. (Reproduced from Defense Intelligence Agency [DIA], *Challenges to Security in Space* [Washington, DC: DIA, 2019], 8, https://www.dia.mil/.)

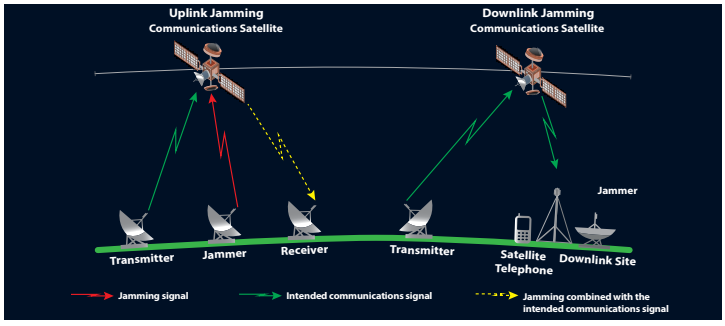

Figure 2. Electromagnetic jamming. (Reproduced from Defense Intelligence Agency [DIA], *Challenges to Security in Space* [Washington, DC: DIA, 2019], 9, https://www.dia.mil/.)

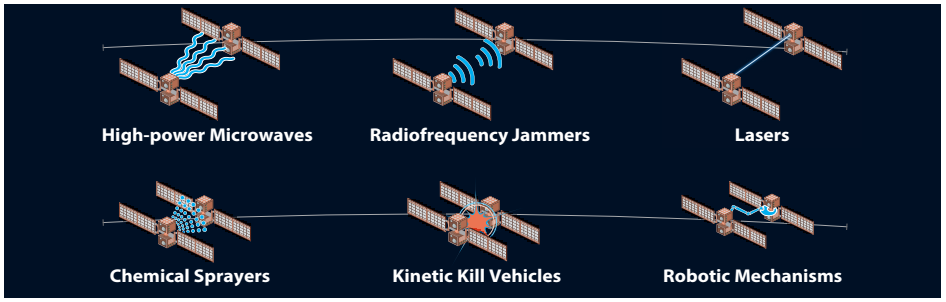

Figure 3. In-orbit satellite-to-satellite threats. (Reproduced from Defense Intelligence Agency [DIA], *Challenges to Security in Space* [Washington, DC: DIA, 2019], 10, https://www.dia.mil/).

As figure 3 demonstrates, a number of space-based weapons may be integrated into a satellite, effectively transforming it into a fully offensive form of dual-use technology. Another form of ASAT weaponry was explored in a 1995 study for the US Air Force, which demonstrated how high-power electromagnetic radiation (EMP) could become the future weapon against satellites in geosynchronous orbit.[62] The strategic employment of such zero-debris (ENMOD Convention–compliant) technology could be codified into future space law as a standard complementing the ban of more damaging (likely kinetic) ASAT weaponry.

Today, it is imperative for the US and its allies to defend themselves against satellite attacks in the hope of averting worldwide repercussions and a crippling of military readiness. Such attacks would have an immeasurable impact on civil society and the military, which depending on the extent of the attack would cause societies to *shut down*—as demonstrated by the May 1998 malfunction of the Galaxy IV satellite.[63] With satellites facing ever greater threats from rapidly advancing ASAT capabilities, it is crucial that Washington lead in efforts to develop tomorrow's protections for satellite technologies.

Conclusion

In drafting today's and tomorrow's rules of the road, the United States must encourage international de-escalation while relying on an advanced defensive posture in space. Leading and negotiating from a position of strength, Washington must advance a balanced, defensive capability as "a prerequisite for a credible deterrence."[64] Reminiscent of the Nixon administration's policy of détente, the United States must undergird its position through the enhancement of treaty verification mechanisms and the international monitoring (e.g., the International Atomic Energy Agency) of space programs, both military and civilian.

A variation of this approach was recently described by Brown University researcher Nina Tannenwald as one advancing "stabilizing military activities."[65] In this approach, "stabilizing military activity (such as monitoring of arms control agreements) should be continued, while developing new weapons technologies that upset the strategic balance should be avoided."[66]

Tannenwald's notion of "stabilizing military activities" mirrors the classical notion of mutual restraint or détente in nuclear deterrence theory. In other words, a realistic policy objective for space peace is likely not the outright banning of weaponized systems in space (though a militarization of the cosmos should be discouraged). Rather, it is one based on the deployment of defensive capabilities necessary to enforce treaty compliance and, in the worst-case scenario, to supply a crucial response to any form of aggression. In fact, it can reasonably be entertained that the drafters of the OST did not prohibit arms deployment in space *sensu stricto* for this exact reason.[67] The deployment of defensive arms capabilities can serve for stabilizing (i.e., defensive) purposes as a crucial set of resources for the protection and effective guarantee of satellite immunity—a policy fundamental to upholding the prohibition of "interference with national technical means (treaty verification satellites)."[68] In this vein, a defensive military presence in space remains central to the preservation of peace through the verification of present and future space arms treaty compliance.

Arms treaty compliance through satellite imagery, as a form of Tannenwald's defensive stabilization, was first introduced through the employment of national technical means (NTM) of verification used by both the US and USSR in mutual compliance verification of the 1972 ABM Treaty.[69] With the legal protection for NTM formally established into law through the 1991 START Treaty, military and civilian satellite immunity have proven fundamental to ensuring compliance with arms control treaties and remain as such to this day.[70] An enhanced protection for NTM of verification, backed by a strong defensive posture in space, will be instrumental in guaranteeing the mutual restraint discussed by both Tannenwald and Gallagher—a model that can continue to inspire the United States, Russia, and China to cooperate on space arms control.[71]

While this optimistic scenario may appear untenable to some, recent experience suggests that cooperation between space powers is more realistic than some strategists have suggested.[72] A striking example of cooperation was seen between American and Russian astronauts during the political standoff between the two countries over the 2015 Ukraine crisis.[73] This remarkable hallmark of international cooperation in space demonstrates

the possibility for the advancement of existing space law as well as the creation of new international legislation that underwrites the continued state practice of free and peaceful international exploration as embodied by the International Space Station (ISS). As US senator Albert Gore Sr. alluded to in 1962, acceptable space operations can indeed simultaneously be "military" and "nonaggressive." In other words, "the test of any space activity must not be whether it is military or non-military, but whether or not it is consistent with the United Nations Charter and other obligations of international law."[74] These prescient considerations are a valuable springboard for future negotiation and the maintaining of peace in the space environment.

In light of these considerations, Washington must prioritize cooperation while remaining skeptical of Chinese and Russian proposals for both a complete or partial weapons ban. A complete weapons ban was initially suggested by the two parties in a working paper submitted to the Conference on Disarmament (CD/1778) in 2006, which was followed by the proposal for a partial weapons ban in the draft 2014 Treaty on the Prevention of the Placement of Weapons in Space, aka the PPWT. While the PPWT's calls for a partial weapons ban may seem reasonable to some, the treaty proposed a ban just for on-orbit weapons and did not address ground-based ASAT weapons—a loophole that fueled international skepticism and ultimately led to the proposed treaty's failure. Perhaps unsurprisingly, the activities of these powers—from China's 2007 *Fengyun 1C* satellite incident to Russia's evolving PL-19 program—foundationally undermine their credibility in committing to a completely or even partially deweaponized space environment. Referring specifically to Russia, though equally applicable to China, US Air Force attorney Christopher Petras contends that "given the extensive history of Russian military utilization of outer space under both the Soviet regime and succeeding administrations, the Russian Federation's current musing about the demilitarization of space could reasonably be looked upon with skepticism."[75] Petras is referring to Russian (and formerly Soviet) thinking from the 1980s to the early 2000s and not the PPWT. Nevertheless, proponents of demilitarization must remain aware that "a regime promoting a purely nonmilitary approach to outer space"—similarly to the weapons ban espoused in the PPWT—"would likely be purely aspirational, lacking clear definitions or compliance measures."[76] In fact, "given the widespread use of space for surveillance and communication, the banning of all military activity in space is, in any case, a wholly impractical option."[77]

Following these conclusions, US national security interests are most likely advanced through the crafting of a defensive American military posture supportive of mutual restraint and, most importantly, through the enhancement of international space law. Strengthening diplomatic channels through the Conference on Disarmament and other international forums of diplomacy is a first, crucial step in the establishment of a codified *jus in bello spatialis* framework. As an important venue for the negotiation of historic arms control agreements and modern-day nuclear policy, the CD can play a vital role in limiting and codifying military operations in space. Providing further specificity and codifying the conduct of military space operations in the form of new, relevant treaty law will help establish modern precedent and a path for lasting peace in the space environment. From arms control to the rules of engagement and conflict resolution, it is imperative that continued arms control efforts be made through a treaty-driven framework. Doing so will strengthen the historic OST while providing a set of solutions appropriate for the challenges of today and tomorrow.

In today's space age, the United States can and must spearhead cosmic diplomacy. After all, enhancing tomorrow's normative space security framework is the only guarantee that "the dream of yesterday is the hope of today and the reality of tomorrow."[78] SSQ

Fabio van Loon

Fabio van Loon is an independent researcher and journalist based in Washington, DC, with an interest in US space policy, European affairs, and international law. An MA candidate for the master of international policy at Texas A&M's Bush School in Washington, DC, and a graduate of LUISS University in Rome, he has had foreign policy research experiences with The Heritage Foundation, the American Enterprise Institute, and the Rome-based foreign policy review *Atlantico Quotidiano* for which he currently writes.

Notes

1. Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Portland, OR: Frank Cass, 2002), 147.

2. Dandridge M. Cole and Donald W. Cox, *Islands in Space: The Challenge of the Planetoids* (Philadelphia: Chilton Books, 1964), 147.

3. *Customary law* is best defined as a form of international law in which international obligations are based on state practice and not explicitly on written conventions or treaties, as in the case of treaty law. A norm becomes a part of customary law when it is first supported by the practice and statecraft of most recognized states and is simultaneously accepted as *opinio juris*, "denot[ing] a subjective obligation, a sense on behalf of a state that it is bound to the law in question." See Cornell Law School's *Wex Legal Dictionary*, s.v. "opinion juris," accessed 14 December 2020, https://www.law.cornell.edu/.

4. Dwight D. Eisenhower, Letter to Nikolai Bulganin, Chairman, Council of Ministers, U.S.S.R., 12 January 1958, online by Gerhard Peters and John T. Woolley, The American Presidency Project, accessed December 2020, https://www.presidency.ucsb.edu/.

5. Outer Space Treaty, Art. 1, 1967.

6. Jackson Maogoto and Steven Freeland, "The Final Frontier: The Laws of Armed Conflict and Space Warfare," *Connecticut Journal of International Law* 23, no. 1 (2007): 27.

7. Daniel Goedhuis, "Some Suggestions Regarding the Interpretation and the Implementation of the United Nations Outer Space Treaty of 13 December 1966," paper presented at the Third World Conference on World Peace Through Law, 1967, quoted in K. Mačàk, "Silent War: Applicability of the *Jus in Bello* to Military Space Operations," *International Law Studies* 94 (2018): 14, https://digital-commons.usnwc.edu/.

8. Malcom Russell, "Soviet Legal Views on Military Space Activities," quoted in *National Interests and Military Use of Space*, W. J. Durch, ed. (Cambridge, MA: Ballinger, 1984), 209.

9. Commission to Assess United States National Security Space Management and Organization, *Report to the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: Commission, 2001), 36, https://aerospace.csis.org/.

10. "US Speech on Outer Space," 30 May 2002, The Acronym Institute for Disarmament Diplomacy, http://www.acronym.org.uk/.

11. Bruce A. Hurwitz, *The Legality of Space Militarization* (Amsterdam: Elsevier Publications, 1986), 67.

12. Hurwitz, 74; and Delbert D. Smith, *Space Stations: International Law and Policy* (New York: Avalon Publishing, 1979), 150.

13. S. P. Sharma, "International Law of Outer Space: A Policy-Oriented Study," *Indian Journal of International Law* 17 (1977): 186, quoted in Hurwitz, *Legality of Space Militarization*, 74.

14. M. Mateesco-Matte, "Space Militarization and Space Law at a Time of 'Non-Peaceful' Coexistence," *Annals of Air & Space Law* 9 (1984): 373.

15. Daniel G. Goedhuis, "The Problems of the Frontiers of Outer Space and Air Space," in *Collected Courses of the Hague Academy of International Law* 174 (1982): 383, accessed 4 December 2020, http://dx.doi.org/10.1163/1875-8096_pplrdc_A9789024728008_03, first published online 1982.

16. Jackson Nyamuya Maogoto and Steven Freeland, "Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?," *International Lawyer* 41, no. 4 (Winter 2007): 1093, http://www.jstor.org/. A further clarification on the OST's permissibility of defensive force in space is this: While the OST clearly doesn't endorse or support the use of weapons in space, the argument that non-WMD weaponry can be used by states lies upon the legal theory of the Lotus criteria. That is, if something is not banned, it is by default legal. The acceptance of the Lotus criteria in interpreting the OST, and generally the treaty law at large, is very much debated to this day. The author's assertion that the OST permits the use of non-WMDs relies on this rationale—particularly in the fact that the OST specifically addresses WMDs but does not rule on the use of non-WMDs while explicitly outlining the *right to self-defense*.

17. P. K. Gleeson, *Legal Aspects of the Use of Force in Space* (Montreal: Institute of Air and Space Law, 2005), 78.

18. S. Aoki, *Routledge Handbook of Space Law* (Routledge: New York, 2017), 199.

19. Jodi Sorensen, "Space Law: The Outer Space Treaty Turns 50!," *Spaceflight News*, 30 January 2017, http://spaceflight.com/; and Eisenhower, Public Papers of the Presidents of the United States, 82.

20. Nina Tannenwald, "Law Versus Power on the High Frontier," *Yale Journal of International Law* 29, no. 2 (2004): 379.

21. 1967 Outer Space Treaty, para. 4, preamble.

22. E. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Portland, OR: Routledge, 2005), 94.

23. Hurwitz, *Legality of Space Militarization*, 73.

24. Louise Dowald-Beck, "San Remo Manual on International Law Applicable to Armed Conflicts at Sea," *International Review of the Red Cross*, no. 309 (November/December 1995), 601, https://www.loc.gov/. Also quoted in K. Mačàk, "Silent War," 17.

25. The Convention on the Law of the Sea, 10 December 1982, 1833 U.N.T.S. 397, enacted as: entered into force as the "United Nations Convention on the Law of the Sea" on Nov. 1, 1994, US Navy Judge Advocate General's Corps, accessed December 2020, https://www.jag.navy.mil/.

26. Bruce Carlson, "Protecting Global Utilities: Safeguarding the Next Millennium's Space-Based Public Services," *Aerospace Power Journal* 14, no. 2 (Summer 2000): 37–38, https://apps.dtic.mil/.

27. Aoki, *Routledge Handbook of Space Law*, 221.

28. Mačàk, "Silent War," 8; and M. D. Ovios, "Rules of Engagement for Space: Where Do You Start?," Faculty of the Naval War College, 2003, 10.

29. McGill Center for Research in Air and Space Law, "About MILAMOS," *Manual on International Law Applicable to Military Uses of Outer Space*, accessed December 2020, https://www.mcgill.ca/.

30. Mačàk, "Silent War," 10.

31. "Chapter V: Peremptory norms of general international law (*jus cogens*)," in United Nations, *Report of the International Law Commission*, Seventy-first session (29 April–7 June and 8 July–9 August 2019) (New York: United Nations, 2019), 142, https://legal.un.org/.

32. Mačàk, "Silent War," 22.

33. Mačàk, 22.

34. NASA, "Nuclear Weapon Effects in Space," accessed December 2020, https://legal.un.org/.

35. R. Ramey, "Armed Conflict on the Final Frontier: The Law of War in Space," *Air Force Law Review* 48 (2000): 152.

36. Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Annex, 1967, https://www.unoosa.org/.

37. Ramey, "Armed Conflict," 150.

38. Mačàk, "Silent War," 31.

39. Mačàk, 32.

40. Ramey, "Armed Conflict," 151.

41. 1907 Hague Convention, Annex, Art. 1, https://ihl-databases.icrc.org/ihl/.

42. Michael Bourbonnière, "*Jus in Bello Spatialis*," in *Space Manufacturing 12: Challenges and Opportunities in Space: Proceedings of the Fourteenth SSI/Princeton Conference on Space Manufacturing*, May 6–9, 1999, ed. Bettie Greber (Washington, DC: American

Institute of Aeronautics and Astronautics; Princeton, NJ: Space Studies Institute, 1999), 147, https://space.nss.org/.

43. Ramey, "Armed Conflict," 153; and Bourbonnière, "*Jus in Bello Spatialis*," 147.

44. Bourbonnière, 147.

45. Bourbonnière, 148.

46. CD/726 (19 August 1986), para. 28; CD/833 (25 April 1988), paras. 25–26; and CD/956 (4 September 1989), para. 52.

47. Aoki, *Routledge Handbook of Space Law*, 222.

48. Protocol Additional to the Geneva Conventions of 12 August 1949 (AP I), Art. 1, Art. 57, 1977, https://www.icrc.org/.

49. Bourbonnière, "*Jus in Bello Spatialis*," 147; Aoki, *Routledge Handbook of Space Law*, 222; and M. Schmitt, "International Law and Military Operations in Space," in *Max Planck Yearbook of United Nations Law* 10 (2006): 89, 116.

50. Aoki, *Routledge Handbook of Space Law*, 223.

51. Aoki, 223.

52. Environmental Modification Treaty, Art. 3(1), Art. 1(1).

53. Aoki, *Routledge Handbook of Space Law*, 223.

54. Bourbonnière, "*Jus in Bello Spatialis*," 145.

55. Bourbonnière, 145.

56. Kendall Russell, "Satellite Launches to Increase Threefold over the Next Decade," *Satellite Today*, 12 October 2017, https://www.satellitetoday.com/.

57. Brian G. Chow, "Stalkers in Space Defeating the Threat," *Strategic Studies Quarterly* 11, no. 2 (Summer 2017): 85, https://www.airuniversity.af.edu/.

58. Defense Intelligence Agency (DIA), *Challenges to Security in Space* (Washington, DC: DIA, 2019), 10, https://www.dia.mil/.

59. CD/726 (19 August 1986), paras. 25–26, 28; CD/833 (25 April 1988), para. 52; CD/956 (4 September 1989); CD/777, 31 July 1987; and CD/786, 24 August 1987, para. 44.

60. 1907 Hague Convention, Annex, Art. 8, https://ihl-databases.icrc.org/.

61. Aoki, *Routledge Handbook of Space Law*, 224; and Ovios, "Rules of Engagement for Space," 14.

62. Maogoto and Freeland, "Space Weaponization," 1112.

63. Ovios, "Rules of Engagement for Space," 16.

64. Chow, "Stalkers in Space," 105.

65. Tannenwald, "Law Versus Power," 413.

66. Tannenwald, 413.

67. "Dr. Robert H. Goddard, American Rocketry Pioneer," NASA, Goddard Space Flight Center, accessed December 2020, https://www.nasa.gov/.

68. Tannenwald, "Law Versus Power," 416.

69. ABM Treaty, Art. 12, paras. 1–2.

70. "U.S.-Russian Nuclear Arms Control Agreements at a Glance," fact sheet, Arms Control Association, accessed December 2020, https://www.armscontrol.org/.

71. "Self-defense" is to be strictly interpreted as the defensive actions taken in accordance with the Caroline criteria and, more broadly, the traditions of Westphalian statecraft.

72. Max Delany, "Feud on Earth but Peace in Space for U.S. and Russia," Phys.org, 26 March 2015, https://phys.org/news/.

73. Delany.

74. Statement of Senator Albert Gore Sr., UN General Assembly, "First Committee Verbatim Record of the Twelve Hundreth and Eighty-Ninth Meeting," U.N. Doc. A/C. 1 /PV. 1289, 3 December 1962, https://www.unoosa.org/.

75. C. M. Petras, " 'Space Force Alpha': Military Use of the International Space Station and the Concept of 'Peaceful Purposes,'" *Air Force Law Review* 53 (2002): 177.

76. Tannenwald, "Law Versus Power," 414.

77. Tannenwald, 377.

78. "Dr. Robert H. Goddard."

PERSPECTIVE

Deterring, Countering, and Defeating Conventional-Nuclear Integration

Justin Anderson
Lt Col James R. McCue, USAF

Abstract

Potential US adversaries have integrated nuclear weapons into their concepts for fighting and winning a future regional conflict. To this end, they have organized, trained, and equipped nuclear-capable forces for theater war fighting. The United States, and its allies, must prepare for adversaries who integrate conventional and nuclear arms to shape the regional battlespace, counter theater defenses, and combat coalition forces. The challenge posed by this conventional-nuclear integration (CNI) cuts across strategic, operational, and tactical levels of warfare. While CNI is not a new phenomenon, its growth and evolution in recent years is placing increasing pressure on US regional deterrence and defense strategies. To effectively deter this threat requires an integrated, but not mirror-imaged, approach. The goal of US CNI is to convince potential adversaries that integrating conventional and nuclear-capable forces grants insufficient advantages within a future regional conflict to overcome either the latter's potential vulnerabilities or the risks attendant with attempting to leverage nuclear escalation. Potential adversaries are likely to retain some of these platforms and their associated nuclear weapons as a hedge against uncertainty. However, it is important for the Department of Defense to bolster US and allied deterrence postures in Europe and the Asia-Pacific by taking steps—prior to any regional crisis—to influence their cost-benefit calculus in contemplating the deployment or employment of nuclear weapons in theater. This article proposes a three-part framework using the Department of Defense's *Deterrence Operations – Joint Operating Concept* (deny benefits, impose costs, and encourage restraint) to plan and posture for accomplishing this goal.

*****

Russia, China, and North Korea are fundamentally opposed to regional security arrangements currently underpinned by US defense commitments.[1] They are determined to undermine these

alliances and partnerships and are preparing for potential future regional conflicts with the United States and its allies. They recognize, however, that US and allied militaries represent a formidable challenge when fighting together with full national support. To counter these forces, potential adversaries seek to fully integrate all elements of their military power, sow political division between Washington and allied capitals, and exploit potential seams and gaps within US and allied theater defense postures.

An important component of their approach is integrating conventional and nuclear-capable forces into their political-military strategies. For advanced militaries, nuclear-capable forces include delivery systems that are solely devoted to a nuclear role and dual-capable platforms that can carry either conventional or nuclear weapons (and whose status and armaments may be unclear to a potential opponent). All three states have developed and deployed both long-range "strategic" nuclear-armed missiles and theater-range (i.e., short-, medium-, or intermediate-range) nuclear-capable delivery systems, with the latter serving alongside, or intermixed with, their conventional forces.[2] These integrated forces provide these actors with the ability to develop combined arms theater campaign plans bringing conventional and nuclear capabilities to bear against US and allied forces within a future potential regional conflict.[3] As stated by Brad Roberts, former deputy assistant secretary of defense (DASD) for nuclear and missile defense policy, the "United States must expect that nuclear weapons would play a role in regional wars against Russia or China," as both Moscow and Beijing have incorporated nuclear coercion, and potential employment, into their "theories of victory" for these types of conflicts.[4] Roberts further assesses that North Korea's nuclear weapons and missile development programs may have granted it "operationally attractive" options for a "credible anti-access area-denial strategy" against the United States and South Korea within a future conflict on the Korean Peninsula.[5] Keith Payne, who also previously served in this DASD role, shares many of these same concerns. In 2018 he noted, "We must understand how to deter Great Powers and nuclear-armed Rogues from exploiting limited nuclear threats and/or escalation for coercive purposes in support of their respective goals to change established orders and borders in Europe [and] Asia."[6]

For US policy makers, it is important to recognize that present efforts to address the challenge posed by conventional-nuclear integration (CNI) can be informed by the Cold War, when the Soviet Union attempted to utilize a combination of conventional forces and theater-range nuclear delivery systems to threaten and attempt to fracture the North Atlantic Treaty Organization (NATO).[7] The United States met this challenge with

its own integrated conventional-nuclear force, with the allied regional defense posture relying on the US arsenal of "non-strategic" nuclear weapons to counter the Warsaw Pact's significant advantage in conventional forces.[8] Critically, however, the present CNI threat from adversaries combines both of these concepts. Russia, China, and North Korea field integrated forces to challenge US regional defense alliances and deterrence postures while also viewing CNI as necessary to offset what they assess as contemporary US advantages in conventional forces.

As a result, while aspects of the present situation echo the Cold War, today's CNI environment is more complex than in the past era. The United States must address the challenge of three potential adversaries fielding integrated conventional and nuclear forces, to include new theater-range, nuclear-capable mobile missiles recently fielded by each state. Our proposed counter-CNI strategy seeks to adapt to today's multipolar context, a half century of technological achievement, and the important fact that the United States is less reliant on nuclear weapons to impose costs on an opponent's military forces within future regional conflicts than its potential adversaries. US policies and strategies for countering the evolving and cross-cutting CNI threat thus requires an integrated, but not mirror-imaged, response. It should leverage US conventional and nuclear-capable forces to enhance regional deterrence and defeat options, without mimicking potential adversaries by overly and dangerously relying on the threat or use of nuclear weapons in theater to prevail in a potential future regional conflict.

This article begins by defining the broader phenomenon of CNI and the present CNI threat posed by Russia, China, and North Korea. Next, it assesses why these potential adversaries seek to integrate their conventional and nuclear-capable forces and how these states may seek to use them in regional crises and conflicts. It then uses the concepts within the DOD three-part framework from *Deterrence Operations – Joint Operating Concept* (deny benefits, impose costs, and encourage restraint) to propose potential courses of action for countering this evolving threat.[9] The US military must prepare for adversaries to readily accept and leverage nuclear risk to realize an advantage in a future regional conflict. With adversary CNI posing a number of pressing challenges to US and allied defense policies and postures, we focus our assessments and recommendations on steps US policy makers and combatant commanders can take to bolster regional deterrence and assurance strategies. These include preparing US war fighters to combat and defeat an opponent's integrated conventional and nuclear forces while signaling preparedness and resiliency to potential adversaries.

Defining the CNI Phenomenon and Present Threat

CNI is a subset of the broader phenomena of nuclear-conventional "entanglement," a term referring to the ways and means by which conventional and nuclear forces may intersect, interconnect, and/or overlap.[10] Importantly, entanglement does not necessarily attribute intentionality to this interrelationship. Research on this subject often focuses on areas of entanglement that may be unintentional and, therefore, are either reversible or can be otherwise addressed to reduce the risk that overlap could lead to nuclear crisis or conflict.[11]

We define *CNI* as the deliberate, calculated decision by a state actor to combine conventional and nuclear-capable forces for the purpose of realizing strategic, theater, and/or tactical military objectives that it assesses cannot be achieved through the use of conventional forces alone. This intentionality extends across a spectrum of activities associated with fielding military forces. These include researching and developing delivery systems and weapons that can fit into an integrated force (such as dual-capable missiles that can carry conventional or nuclear warheads); organizing, training, and equipping both conventional and nuclear-capable military forces; preparing, planning, and training these forces to operate together; and openly conducting tests or exercises for combined operations, demonstrating how one type can support or enable the other and/or making clear to outside audiences that nuclear-capable forces are integral to theater war-fighting concepts. The focus here is on the integration of conventional and nuclear-capable forces by Russia, China, and North Korea as actors that represent potential adversaries of the United States. It is important to note, however, that CNI is a broader phenomenon that also extends to states such as Pakistan, which has integrated short- and medium-range nuclear-capable forces into strategies and plans for defending its territory against a potential cross-border offensive by large numbers of Indian conventional forces.[12]

Understanding the Evolving CNI Threat

While the integration of nuclear and conventional forces never fully disappeared after the end of the Cold War (to include for the purposes of preparing for potential regional contingencies), CNI has substantively evolved in the past five years in a manner posing additional threats and challenges to the United States and its allies.[13]

Russia, China, and North Korea have devoted significant resources to developing and fielding new theater-range, nuclear-capable delivery sys-

tems. Their goal is to supplement their conventional forces and to provide their national leaders with options for threatening regional states and holding US and allied targets at risk below the threshold of strategic nuclear forces. Russia deliberately violated the Intermediate-Range Nuclear Forces Treaty that reflected US-Russian mutual agreement to fully eliminate an entire class of missiles and reduce the risk of regional nuclear crises. It did so by developing and fielding the SSC-8/9M729, a dual-capable, ground-launched intermediate-range cruise missile—the exact type of delivery system expressly banned by the treaty. As stated in November 2018 by then-director of national intelligence Dan Coats, Russia now fields "multiple battalions of 9M729 missiles, which pose a direct conventional and nuclear threat against most of Europe and parts of Asia."[14] The missile joins a range of other Russian short- and medium-range nuclear-capable delivery systems (ground, naval, and air) that can be equipped with munitions from the country's "active stockpile" of approximately 2,000 "non-strategic nuclear weapons."[15] China currently fields the world's largest arsenal of medium- and intermediate-range conventional and nuclear-capable missiles.[16] While Beijing long restricted its nuclear forces to a relatively small number of silo-based intercontinental ballistic missiles kept at a low level of readiness, it now deploys multiple mobile nuclear-capable delivery systems.[17] These include the DF-26, an intermediate-range ballistic missile (IRBM) that the Chinese media describes as having an "aircraft carrier killer" role and the DOD states is "capable of rapidly swapping conventional and nuclear warheads" and ranging US bases across the Indo-Pacific region as far as Guam.[18] In addition, North Korea has pursued a breakneck effort to develop a range of conventional and nuclear-capable missiles, to include theater-range, nuclear-capable systems such as the KN-15 MRBM and Hwasong-12 IRBM. Pyongyang has successfully test-launched both missiles from transporter erector launchers (TEL), leading a number of analysts to conclude these systems are either operational or will be in the near future.[19] Moreover, Russia and China, per unclassified US government assessments, maintain open production lines for nuclear weapons (with China potentially doubling its nuclear arsenal in the next decade), while North Korea has stated it maintains the ability to produce fissile material for new weapons.[20] The implications of such developments are that Russia, China, and North Korea have intermingled their conventional and nuclear-capable forces.

Russia, for example, currently deploys several SSC-8/9M729 IRBMs together with its conventional forces (to include conventionally armed ballistic missiles) stationed in the Kaliningrad Oblast bordering Poland

and Lithuania, where these missiles can range a number of key NATO military facilities across several states.[21] China's People's Liberation Army Rocket Force (PLARF), responsible for the country's ground-based missile fleet, assigns brigades of conventional and dual-capable delivery systems to shared bases, appears to deploy and/or exercise these brigades in overlapping areas, and is increasingly training its personnel in how to use both.[22] This situation led at least one PLARF officer to publicly note the increased burden in training, stating in 2017 that "our missile weapon systems are both nuclear- and conventional-capable. . . . Nuclear must be learned, and conventional also must be learned. This is equivalent to one person doing two jobs."[23] China's command-and-control systems and processes for conventional and nuclear-capable missiles also appear to be either shared or substantively overlap.[24] In addition, North Korea's conventional, dual-capable, and nuclear missile programs are closely integrated, both in terms of "systems integration" and in some cases, colocation at certain bases.[25]

Russia, China, and North Korea have also conducted exercises and/or tests where nuclear-capable forces carry out strikes demonstrating their ability to support a broader, integrated force in its achievement of regional war-fighting objectives. From 2013 to the present, several Russian military exercises have combined conventional and nuclear-capable forces in operations practicing for an armed conflict against an unnamed adversary that appears closely modeled on NATO. These exercises have included "simulated" nuclear attacks against NATO members and partners and tests of various types of nuclear-capable systems in providing fire support to conventional forces.[26] In August 2020, China made public a recently concluded "cross regional confrontational exercise," allegedly held in response to the "US provocatively [sending] two aircraft carriers to the South China Sea for exercises [with] India, Japan and Australia" that practiced striking mobile targets at sea, such as aircraft carriers.[27] This exercise followed a number of other PLARF exercises highlighted by Chinese government-controlled media outlets in the last four years that have featured theater-range, nuclear-capable missile units rapidly deploying and carrying out simulated strike operations against an advanced military opponent equipped with fighter jets and "electronic warfare" capabilities (which in at least one case was directly referred to as the "blue team" squaring off against the PLA's "red team").[28] North Korea has stated that past tests of its nuclear-capable missiles represent practice for potential future strikes against US military bases in Japan.[29] These tests (and statements) are consistent with both South Korean and US assessments of North

Korea's strategy for a future conflict on the peninsula, which would first rely on "coercive nuclear preemptive threats" with ballistic missiles to try to prevent unified US and allied action against its forces.[30] If these threats failed to have the desired effect, Pyongyang would then lean on artillery and missile strikes, to possibly include with nuclear weapons, against Seoul and US bases in South Korea and Japan to support a surprise attack by its conventional forces to attempt to win a quick victory prior to the arrival of US reinforcements.[31]

In short, these above developments reflect the DIA's 2018 assessment that Russia, China, and North Korea are developing and fielding nuclear capabilities "for military or coercive use on the battlefield." All three states view integrated forces—and the credible threat of nuclear employment on regional battlefields by theater-range platforms—as important to their "theories of victory" for future potential regional conflicts.[32]

Why Pursue CNI?

Development of capability alone, however, does not fully explain the intent of potential adversaries or the potential risks CNI poses to the United States and its allies. Why have Russia, China, and North Korea pursued CNI, and why should their integration of conventional and nuclear-capable forces concern the United States?

Russia, China, and North Korea's perspective on regional affairs represents a jaundiced form of realism; while they strongly believe they are engaged in a "zero sum game" with the United States and its allies (with regional prestige and influence the prize), they categorically reject ever accepting a regional balance of power.[33] Russian and Chinese leaders are determined to be seen both at home and abroad as the preeminent power within their respective regions (with North Korea's primary concern that it be recognized as the strongest state on the Korean Peninsula and a power center independent from the United States and China).[34] All three thus strongly oppose and continually seek to undermine US-led regional security arrangements, which Russia and China view as obstacles to assuming their "rightful" place as first among equals in the region. Meanwhile, North Korea fears that US allies such as Japan will wholeheartedly support Washington's efforts to topple its ruling regime.

This competitive animosity leads these states to contemplate and prepare for potential armed conflict with the United States and its allies either on or near their borders or within what they view as their traditional sphere of influence. All three likely assess that they face a significant challenge in defeating the United States and its regional allies within a conflict

that solely features conventional forces. They worry that US conventional forces will best their own in a future fight and fear facing the same type of ignominious defeats meted out to autocrats such as Slobodan Milosevic and Saddam Hussein in past conflicts.[35] Moreover, they are deeply wary of launching any kinetic strike against the US homeland, likely calculating this type of attack would bring the full force of the United States to bear on a conflict they would prefer remain regional.

Russia, China, and North Korea thus conclude they face a significant security dilemma in their pursuit, within their respective regions, of what they consider critical national objectives. They believe it imperative to field and wield military power that can coerce and compel other regional states to accept their leadership. At the same time, however, they seek to limit US involvement, and prevent US intervention, in regional affairs, to include within any military crises or conflicts. Moreover, they are committed to preparing for a possible future fight with the United States or its allies and resolve to find a potential pathway to victory either on the battlefield or at the negotiating table.[36]

We assess that Russia, China, and North Korea conclude that integrating conventional and nuclear forces, with the latter specifically featuring theater-range options, can play a key role in achieving these imperatives. CNI does so, in their view, by allowing their military forces to realize some or all the following objectives within a potential regional conflict with the United States and its allies.

To Guarantee at Least a Draw (and Thus Preserve the Regime)

Russia, China, and North Korea all view military power as a critical tool of statecraft and seek to use it to coerce and compel other states. All three are wary, however, of the risks of military aggression against the United States and its allies. They do not have full confidence of victory in a regional conventional military conflict. Moreover, their leaders may fear that suffering a serious military reversal in the field could pave the way for US-imposed regime change or even catalyze an internal coup d'état.[37]

In the face of these grim (but in their view, entirely plausible) outcomes, Russia, China, and North Korea likely view theater-range, nuclear-capable forces as critical to preventing potential setbacks within a future regional military conflict from turning into routs. They may conclude that the only means to force the conclusion of an armed conflict not going their way is to threaten US and allied forces with a theater nuclear strike unless both sides agree to a cease-fire and/or a negotiated settlement.[38] Should this fail to end hostilities (and if their conventional forces continue to suffer

reverses in the field), they may seriously contemplate employing a theater nuclear strike against US and allied forces, perhaps even on or within the boundaries of their own borders to cover a military retreat. They may gamble that nuclear employment in the midst of ongoing combat—perhaps with a small number of weapons configured for low yield and low fallout—would fall below the threshold of the US stated policy to impose "intolerable costs" in response to an adversary's nuclear attack.[39]

Their leaders very likely understand that a nuclear strike causing significant US or allied civilian casualties would result in devastating counterstrike. But in the heat of a battle with potentially existential stakes, they may bet that a "limited" nuclear attack on US or allied military forces—particularly if these forces were either afloat or away from major civilian population centers—might be assessed differently by US leaders. All three states may share the assessment of Bernard Brodie, who in his 1965 classic, *Escalation and the Nuclear Option,* concluded that "the use or threat of use of nuclear weapons in tactical operations seems at least as likely to check as to promote the expansion of hostilities."[40] Like the venerable Cold War strategist, they may conclude that theater nuclear employment will not necessarily result in a broader nuclear war, as the attacked party may hesitate to order a significant nuclear counterattack for fear of initiating a mutually destructive nuclear conflagration. If so, this form of nuclear employment may be viewed as an acceptable risk and the best, or perhaps the only, way to halt the advance of coalition forces and compel the United States and its allies to accept a negotiated settlement.[41]

To Discourage Allied Participation and/or US Intervention

Any future regional crisis or conflict involving Russia, China, or North Korea will occur near their borders and under a nuclear shadow cast by their growing nuclear arsenals. Potential adversaries may view CNI's ability to put pressure on US alliances as one of its prime benefits, forcing foreign leaders to contemplate the possibility that their populations and military forces can be targeted with nuclear-capable platforms from the outset of hostilities. CNI allows Russia, China, and North Korea to exercise or deploy large integrated conventional-nuclear forces—prominently featuring theater-range, nuclear-capable delivery systems—adjacent to allied territory.

Russia and North Korea, for example, have already made open, credible nuclear threats against allied targets in Europe and the Asia-Pacific, respectively. In addition to the simulated nuclear attacks against NATO noted above, Russian officials and legislators have made public nuclear

threats against NATO allies and partners for their support of activities such as theater missile defense exercises and hosting US forces.[42] North Korea regularly makes bellicose nuclear threats against US regional allies, to include stating that Japan's main islands can be "sunken into the sea" with nuclear weapons and that South Korea faces "pre-emptive" and "indiscriminate" nuclear attacks due to its ongoing military cooperation with Washington.[43] These statements aim to dissuade key allied and partner capitals from operating or exercising with the US military and to convince their publics to oppose hosting or otherwise supporting US forces. These shots across the bow may also represent attempts by potential adversaries to influence regional states to consider denying the US military access to airports and seaports in a future conflict, slowing the flow of US forces intended to relieve beleaguered allies into the theater (and possibly tipping the balance of a contested fight).

Adversaries may also view CNI as useful for raising questions in Washington regarding whether overseas allies are worth the potential cost in US blood and treasure necessary to defend them against nuclear threats from delivery systems that cannot range the United States. They may also seek to raise doubts in allied capitals regarding whether a US president would answer these questions in the affirmative. These issues are not new. During the Cold War, Western European leaders perennially asked whether a US president would really "trade New York or Detroit to save Hamburg or Bonn."[44] They are made acute, however, by the evolution and expansion of theater-range, nuclear-capable options and the fact that these capabilities are fielded by multiple actors. Dissuading the United States from military intervention on behalf of allies, and persuading these actors they may be better off negotiating their own forms of bilateral détente, will be top priorities for Russia, China, or North Korea in a future regional military crisis or conflict. All three may view CNI as a way to achieve both objectives.

To Provide Fidelity for (Theater) Brinkmanship

Potential adversaries may also believe that integration grants them a more expansive military tool kit for managing and exploiting future regional crises. They may view CNI as granting ways and means for manipulating nuclear risk in a regional crisis or conflict in a manner that enhances the reach or weight of their conventional forces. Russian military writings, for example, argue that "the threat of nuclear escalation, particularly with nonstrategic nuclear weapons, helps amplify the coercive effect of strategic conventional weapons."[45] The mobility of theater-range, nuclear-capable

platforms that can transit to and from border areas, for example, can provide leaders with a form of local pressure that can be readily dialed up or down against neighboring or nearby states as needed.[46]

Introducing theater-range, nuclear-capable forces into a region and/or spotlighting their presence may also be viewed—by potential adversaries and allies—as a way to ratchet up tensions during a crisis by providing the former with a more plausible battlefield weapon than "strategic" nuclear forces capable of reaching the United States. Saber rattling with the latter would likely prompt the United States to quickly respond with strong deterrence and assurance measures. Potential adversaries may calculate that the ambiguous status of integrated forces in theater permits them to communicate threats with these capabilities that will effectively play on the fears of regional actors without directly antagonizing Washington.[47]

To Complicate the Rules of Engagement (ROE) and Targeting

A potential adversary might also hope that deliberately intermixing conventional and nuclear-capable forces at certain locations, or as part of a specific combined arms operation, will shield the latter and transfer this protection to nearby assets. Its intent is for the United States to either hesitate before launching an attack against an intermixed force or otherwise truncate target lists in a way that limits the effectiveness of strikes.[48] For Russia, China, and North Korea, this ability to buy time, and perhaps a form of protection, for their integrated forces in theater may be considered an important way to achieve a military balance against the United States and its allies. It may also provide a means of safeguarding certain key homeland targets, such as rear-area military headquarters or political leadership sites, from US conventional attacks through stationing nuclear-capable forces at these locations or signaling (or tacitly allowing the US to conclude) that these facilities are integral to the command and control to some or all of their nuclear forces.

This approach relies on potential adversaries making two broad assumptions. The first is that the United States is unable to readily discern the difference between intermixed conventional and nuclear-armed forces in theater. US forces will thus prove wary of engaging the combined forces of an opponent out of concern the possible inadvertent or incidental destruction of nuclear platforms (or their means of command and control) could escalate a conventional fight into a nuclear conflict. The second assumption is that even in those cases where the United States is confident it has correctly identified an opponent's theater-range, nuclear-capable platform, it will hesitate to attack these forces. Recognizing that these

forces represent high-value assets (due to their limited numbers, their value to leadership, or other factors), the United States may fear attacks on these platforms will quickly place an opponent into a "use or lose" situation with its remaining delivery systems.[49]

If these assumptions proved correct, CNI could pose a unique obstacle to US freedom of action regarding attacking key adversary forces, bases, and supporting elements. Potential adversaries are deeply concerned by the speed, accuracy, and effectiveness of US strike capabilities and are eager to find ways and means to counter this advantage. They may view comingling conventional and nuclear-capable forces as useful for slowing or even paralyzing US military activities in the field, complicating US ROEs, forcing US war fighters to gather onerous amounts of information before acting, and/or pushing targeting decisions up the command chain.

To Enhance the Lethality of Standoff Strike Options

Nuclear weapons are uniquely powerful; the effects of detonation include blast, heat, radiation, and an electromagnetic pulse.[50] A nuclear warhead's explosion is orders of magnitude more destructive than a comparably-sized conventional one. By arming theater-range platforms with nuclear weapons, aggressors significantly increase the destructive capacity of their standoff strike options.

This enhanced lethality can boost broad efforts to restrict US and allied freedom of movement in theater that are sometimes collectively referred to as anti-access/area denial (A2/AD) strategies. Adversaries may believe that the threat of a possible nuclear strike in theater will cause US political leaders and military commanders to hesitate before flowing additional forces into a particular region or lead to less efficient, more dispersed force flow. They may also hope the presence and posture of theater-range, nuclear-capable systems on or near their land or maritime borders can force US ground forces to avoid using or transiting through certain areas or US naval forces to keep their distance from coastlines.

Potential adversaries who fear they are overmatched in theater (whether due to US and allied strike systems in particular or some "correlation" of offensive and defensive forces in general) may view the destructive potential of theater-range, nuclear-capable forces as providing a more favorable balance of forces, particularly if they only have limited numbers of standoff strike systems available.[51] In the event of an actual conflict, equipping platforms such as theater-range mobile ballistic missiles with nuclear warheads may also provide an option for delivering a stinging blow against massed coalition forces or other critical targets that are either outside the

reach, or resilient to the effects, of their conventional platforms. At a basic level, nuclear weapons may be the most lethal munitions available to an opposing force, and their use in combat could simply reflect a potential adversary's assessment that military necessity demands their employment.

The above list is not intended to be comprehensive or all inclusive, nor do all these reasons apply to every potential adversary that integrates its conventional and nuclear-capable forces. Several of the above factors, however, likely figure into the decision-making calculus of potential adversaries. Understanding the nuances of why potential adversaries are pursuing CNI is essential for the United States to prepare efficiently and effectively to deter, counter, and defeat these types of capabilities.

Countering the CNI Threat

Adversary CNI poses two interrelated challenges for US policy makers and US combatant commanders. First, Russian, Chinese, and North Korean CNI represents a cross-cutting challenge for US defense policy and military strategy. Their integration of conventional and nuclear-capable forces can affect a range of US and allied cost-benefit calculations before and during hostilities. By placing pressure on US alliances and extended deterrence guarantees, the CNI threat requires US policy makers to devote time and attention to assuring allies they are protected against an opponent's conventional and nuclear forces, to include during any regional contingency or conflict. It also necessitates US policy makers making resource decisions on capability investments, the placement of forces, and other matters relevant to countering potential adversaries in contested regions. Furthermore, it presents a range of operational and tactical issues for US combatant commands that must plan against the challenges posed by an opponent's integrated force, to include the possible threat of nuclear employment in a regional conflict. Moreover, these various challenges cannot be separated from each other. Adversaries and allies must believe the United States has both the political will and military capacity to directly counter, deter, and if necessary, defeat an integrated force fielding conventional and nuclear-capable assets in a regional fight far from US shores.

The second challenge is convincing potential adversaries that theater-range, nuclear capable delivery systems operating as part of an integrated force do not represent a critical offset to, or a competitive advantage against, US and allied forces in a regional conflict. Russia, China, and North Korea likely assess that the stakes of a possible regional armed conflict are higher for them than for the United States. Potential adversaries may view CNI as a useful *cost imposition* strategy vis-à-vis the United

States, prompting US commanders to expend significant time and resources to either defend against or attempt to avoid platforms they are forced to treat as highly lethal war-fighting assets. As described by Kenneth Ekman, "Cost imposition strategies focus on eliciting an adversary response that creates a hardship differential favoring the initiating nation. . . . Necessary preconditions include the requirement and will to compete, the impetus to do so efficiently, and the potential to do so from a position of capability advantage with ability and intent to elicit a disadvantageous response from an adversary."[52] To counter this strategy, the United States must attempt to convince potential adversaries that integrating conventional and nuclear-capable forces will incur rather than impose costs, particularly if they are used to commit regional aggression.

Addressing these two challenges in an era of military competition with Great Powers and ongoing contention with rogue regimes requires renewed policy attention and military focus. Following the approach to deterrence stated in the Department of Defense *Deterrence Operations – Joint Operating Concept*, US policy makers and combatant commanders must work together to affect the "adversary's decision calculus elements in three 'ways': Deny Benefits, Impose Costs, and Encourage Adversary Restraint."[53]

Importantly, due to the unique challenges posed by nuclear weapons, deterrence (and parallel efforts to assure allies) cannot rely on conventional forces alone. The United States needs its own integrated response addressing adversary CNI as a strategic, operational, and tactical threat. Combatant commanders, for example, need to develop plans and activities designed specifically to deter potential adversaries from either integrating their forces or attempting to leverage CNI for the purposes of intimidation, coercion, or armed aggression within a contested region. The Department of Defense recognized this issue in the *2018 Nuclear Posture Review* (NPR) and now requires "the integration of [US] nuclear and non-nuclear military planning. Combatant Commands and Service components will be organized and resourced for this mission, and will plan, train, and exercise to integrate US nuclear and non-nuclear forces to operate in the face of adversary nuclear threats and employment." The NPR further notes that "the United States will coordinate integration activities with allies facing nuclear threats and examine opportunities for additional allied burden sharing of the nuclear deterrence mission."[54]

Critically, however, this integration should counter, but not mirror-image, the CNI strategy of potential adversaries. The latter's approach incorporates CNI as part of broader political and military strategies that ultimately rely on coercion and threats of aggression to reorder regional

security arrangements. In addition, all three states have rejected US offers over the past decade to engage in substantive talks on arms control, strategic stability, or regional confidence-building measures for nuclear or conventional forces.[55] They assert that their increased commitment to nuclear forces (to include theater-range, nuclear capable delivery systems) is necessary to address a dangerous and unstable regional security environment, but for the most part refuse to engage in diplomacy that could address a range of risks associated with military competition, whether with nuclear, conventional, or both types of forces.

In contrast, the US approach to CNI should be carefully calibrated and clearly communicated as a commitment to regional stability that directly denies the benefits, and increases the costs, of nuclear threats and aggression. US CNI can be further differentiated from potential adversaries' approach to integration by emphasizing that, as an important part of the US approach to extended deterrence, it is collaborative in nature, reflecting Washington's readiness to accept risks to defend its allies against all threats. In addition, the United States should continue to press all three capitals to participate in diplomatic talks and military-to-military engagements aimed at verifiably reducing nuclear risks, to include those associated with entanglement, while simultaneously ensuring its force capabilities and posture provide US negotiators with a strong hand in future negotiations. By making these distinctions in the development of a US approach to CNI, policy makers and combatant commanders can ensure the US response to integrated nuclear and conventional threats both assures nervous allies and imposes costs on those choosing to rely on delivery systems such as theater-range, nuclear-capable platforms.

Deny CNI Benefits (Intermingling)

Potential adversaries may believe they can realize a number of benefits from intermingling their conventional and nuclear forces, to include complicating US efforts to understand their order of battle, obscuring the nature and purpose of key strike systems, and even attempting to protect certain locations or units from attack. To deny them from realizing any advantages from either attempting to cloak their intent or shield key assets, the United States should seek to equip military commanders with intelligence, surveillance, and reconnaissance (ISR) capabilities that can help disentangle these integrated forces by identifying the presence of nuclear weapons on the battlefield.

The development and fielding of tools for providing commanders with this information represents a significant, but not insurmountable, techni-

cal and tactical challenge. Past experiments have demonstrated the ability to use standoff platforms equipped with radiation detectors to find radioactive signatures at a distance, to include those associated with nuclear weapons. In 1989 US and Russian scientists, as part of a joint effort to develop verification tools for future nuclear arms control agreements, successfully demonstrated that a helicopter equipped with a neutron detector could find a nuclear weapon stored inside a surface ship from a range of 100–150 meters.[56] Later experiments using detectors carried by piloted and remotely piloted platforms have shown improvement in the ability to detect different types of radiation sources at these and greater distances, to include in radioactively contaminated environments.[57] Although not designed for battlefield conditions, these platforms and their sensors could possibly be modified for military purposes. In addition to providing means for detecting nuclear weapons on a battlefield and depriving potential adversaries the ability to hide or mask the status of delivery systems (or the larger force elements within which they are integrated), these types of platforms could also prove invaluable for finding and securing stored, unused, or even lost nuclear weapons and help support future diplomatic efforts to develop a new generation of arms control agreements.

Deny CNI Benefits (Lethality)

Within potential future regional conflicts, the United States and its allies may face adversaries willing to take significant risks to achieve their goals or to avoid ignominious defeat. A combatant commander facing an adversary with an integrated nuclear and conventional force must prepare for the possibility that it may seriously contemplate a theater nuclear strike even if it is well aware that the United States can impose considerable costs in response.

In addition, potential adversaries may integrate their standoff strike capabilities (such as air and missile platforms) to boost the profile of their overall forces within a regional conflict. In doing so, they may hope to force their opponents to treat some or all of these forces as if they are equipped with nuclear munitions, expending finite time and resources attempting to deal with this amplified risk.

This scenario highlights the importance of the United States developing deterrence strategies to deny a potential adversary from realizing any benefits from launching a standoff nuclear strike in theater against US and allied forces and imposing significant costs should such a strike be attempted during a regional conflict. Such strategies can play a critical role in assuring allies that the United States wields both a sword and a shield

on their behalf against CNI opponents. Deterrence by denial efforts aimed at achieving this goal can include mounting both "active" and "passive" defenses against an adversary's theater-range, nuclear-capable platforms.

Active defenses. The primary US approach to protecting forces from theater air and missile threats is integrated air and missile defense (IAMD).[58] IAMD posits a layered, dynamically active approach to incorporating "sensors and shooters" that brings together radars and theater missile defenses (such as Terminal High Altitude Area Defense [THAAD] and Patriot Advanced Capability [PAC]-3 batteries). This approach is "agnostic" with regard to the characteristics of the armaments of the air and missile platforms it defends against, and US military doctrine on IAMD does not generally focus on or otherwise highlight theater-range, nuclear-capable threats for prioritization, especially during a mass strike.[59]

This approach is both logical and practical in terms of broad application to the wide range of air and missile threats faced by US and allied forces worldwide. Within a region where an adversary has integrated its conventional and nuclear-capable forces, however, US policy makers and combatant commanders can send signals (e.g., via IAMD exercises) communicating to an adversary that it cannot trust that a limited theater nuclear strike will prove successful.[60] In addition, intelligence-based tipping and cueing can help focus "sensors and shooters" on nuclear threats hidden within a larger salvo, focusing interceptors on the most lethal part of an adversary's attempted strike. The realization that even a limited defensive system can plausibly destroy an inbound nuclear-armed missile or aircraft can serve as an important deterrent to potential adversaries launching such an attack. US and allied active defenses can tilt their cost-benefit assessments against attempting a standoff strike whose prospects are uncertain but whose initiation invites major retaliation.

No defense, however, can provide a perfect shield against all incoming attacks. An unfavorable ratio of interceptors against the number of both conventional and nuclear missiles an adversary can fire (and/or air defenses against adversary dual-capable strike aircraft) requires a theater IAMD approach that integrates offensive and defensive operations.[61] During a conflict, for example, ISR systems tracking an adversary's theater-range, nuclear-capable systems could send information about an imminent launch to both missile defense interceptors and piloted and remotely piloted assets already in the air.[62] These latter forces could then undertake actions (both kinetic and nonkinetic) to destroy, disable, or otherwise disrupt adversary air and missile forces before they can fully launch an attack or fire a second salvo, helping to prevent US and allied defenses from being overwhelmed—

even as these latter forces are already alerted to, tracking, and preparing to intercept any missiles that make it into the air.

With this mixed offense-defense approach, the United States and its allies can place and posture forces that can rapidly impose costs on an opponent's launchers and their support elements at the same time as partnering defensive capabilities are denying the benefits of the attempted strike. This can further bolster the United States' deterrence posture against an integrated opponent contemplating a theater nuclear strike, as it may have a limited number of high-end assets such as TELs and strike aircraft—only some of which may be armed with nuclear weapons. If a potential adversary has to worry that any attempt at launching such a strike faces poor odds of success and may well result in some or many of its most prized forces and weapons being knocked out of the fight (perhaps without any prospect of replacing them in time to affect the remainder of the conflict), it may conclude that this type of attack is not worth attempting.

Passive defenses. Another key tenet of a robust regional deterrence posture against a CNI opponent is to convince the potential adversary that US and allied forces can survive—and operate in, around, and through—a potential theater nuclear attack. While less high-profile than active defenses, passive defenses play an important deterrent role against theater nuclear use, particularly if the latter's combined arms operations rely on a handful of standoff strikes against key US and allied nodes either on the battlefield or at operational depth.[63]

If the hardening of key facilities in theater, for example, means that an adversary attack featuring a limited number of low-yield nuclear munitions causes damage at ports and/or bases within the region but does not necessarily suspend all US operations, then the construction of protective structures such as "third generation" hardened aircraft shelters at these locations is a worthwhile investment.[64] Importantly, not all facilities necessarily require hardening, which would prove prohibitively expensive. Selective hardening may be sufficient to protect critical facilities and impact an adversary's cost-benefit calculus, as the latter must factor in the possibility that a nuclear attack may hit but neither fully nor effectively destroy its target.[65] The attack will have thus broken the nuclear taboo, with costly implications, to realize little or no military gain.

In addition, dispersion and redundancy are two means of defeating geographically and numerically limited nuclear threats that may prove more affordable than widespread nuclear hardening. The essential assumption underpinning this counter-tactic is that dispersion and duplication create more targets than the attacker's means of destruction. In the past, force

dispersal posed a challenge to regional combatant commands because this complicated the ability to concentrate combat power. Advances in communications technology and networked approaches to warfare, however, have drastically reduced this negative effect.[66] Integrated command, control, communications, computers, and intelligence (C4I) is a baseline requirement for contemporary theater combat operations. Many core capabilities such as intelligence gathering and munitions delivery are now also naturally disaggregated and dispersed across the fighting force. In addition, precision strike effects can be provided from many ground, air, or sea platforms deployed to the theater. In short, smaller numbers of platforms, operating from a range of locations (to include locations outside of the theater), can now provide the same effects that once required massing forces at a few regional bases.

This message is bolstered by the United States demonstrating the ability to combine assets in and outside of a specific theater to practice complex operations, such as a July 2020 maritime exercise where a B-52 from a US-based bomber task force flew 28 hours to support a US carrier strike group in the Pacific.[67] Publicizing these types of exercises clearly demonstrates to both US allies and potential adversaries that geographic distance is no obstacle to US efforts to rapidly and decisively respond to potential regional aggression. Moreover, this approach may realize a range of efficiencies for the global force, and it would be worthwhile for the Defense Science Board or some other US government-funded research effort to study how dispersion and duplication can help the United States address regional defense and deterrence challenges in an era of Great Power competition.

Exercises simulating nuclear environments against nuclear-armed opponents. Deterrence can be further strengthened by demonstrating competency fighting on simulated radiologically contaminated battlefields. US and allied forces should conduct combined exercises preparing participants to encounter both conventional and nuclear-capable forces on regional battlefields. Moreover, these exercises, whether conducted in theater or on tabletops, should continue unabated through a simulated battlefield nuclear attack. This act should not be treated as a terminal part of the exercise or as an activity separated from other "conventional" actions. Demonstrating preparedness to continue operations despite a notional opponent's theater nuclear strike assures both internal and external actors of the US-led coalition's ability to remain cohesive and effective after any conventional or combined attack.

These types of exercises are critical for both physically and psychologically preparing personnel for a situation without precedent—continuing

to fight following adversary employment of a nuclear weapon. A study of the potential psychological effects of a nuclear attack notes that following the nuclear bombings of Hiroshima and Nagasaki, survivors of the attacks reported, in addition to physical injuries, "psychic numbing, severe anxiety, and disorganized behavior, and there were later chronic effects such as survivor guilt and psychosomatic reactions." The study's author concludes that the psychological impact on military personnel surviving a nuclear strike would likely be the same.[68] While nothing can fully mitigate the shock of experiencing a nuclear attack, preparing forces for the possibility that one could occur on a battlefield where they are engaged in combat can help manage fears of the unknown. Doing so can ensure that, should a nuclear detonation occur, troops are mentally and physically prepared to maintain good order while treating casualties, mitigating radiological contamination, and preparing to execute response orders.[69]

Within a future regional conflict a potential adversary, if sufficiently pressured, may gamble that the "shock value" of a nuclear detonation in theater will provide time, space, and other forms of military advantage. By devoting attention and resources to openly preparing US and allied forces to withstand the physical and psychological impact of a nuclear attack, US policy makers and combatant commanders can clearly signal to an adversary that the United States and its allies will be neither intimidated by nor unprepared for possible nuclear strikes in theater.

Impose Costs

The ability to impose unacceptable costs via defeat in actual tactical combat is also foundational to deterrence theory. As described in the DOD's *Deterrence Operations – Joint Operating Concept,*

> Deterrence by cost imposition involves convincing adversary decision-makers that the costs incurred in response to or as a result of their attack will be both severe and highly likely to occur. Cost imposition includes the full array of offensive operations including kinetic and non-kinetic options. . . . The key challenge to improving the effectiveness of deterrence by cost imposition is to overcome adversar[ies'] perceptions that they can successfully deter US attack, or that the US will be self-deterred.[70]

In addition to making it clear to potential adversaries that their integration of conventional and nuclear forces cannot effectively hide or protect the latter, it is important for the United States to show that it can rapidly target and destroy high-value, low-density, nuclear-capable assets such as mobile missiles. While strike lists within a campaign strategy will

undoubtedly target many other types of assets, these expensive and rare nuclear-capable platforms are an easily justified pressure point for imposing costs in response to the threat or employment of nuclear weapons in theater. Increasing the vulnerability of an adversary's theater-range, nuclear-capable forces will decrease the utility of both CNI in force planning and the use of these forces in theater war fighting.

Calibrate the kill chain. The ROEs and "kill chain" for fighting a CNI adversary will differ in several ways from fighting an opponent that fields a solely conventional force. It is important for policy makers setting guidance (and for combatant commanders in planning and execution) to balance several key considerations. If there are policy and operational concerns regarding attacking nuclear-capable platforms that may or may not be armed with nuclear weapons, US forces in theater should be equipped with precision weapon options that can disable or destroy these threats with low collateral damage risk. Hellfire missiles equipped with blades instead of explosives, for example, are already in the US arsenal; these or other nonexplosive weapons could potentially be used against the crew or tires of a wheeled TEL carrying a missile in order to prevent it from reaching a launch site.[71] In addition, directed-energy weapons (DEW), several of which are in later stages of development, may provide other nonexplosive options for disabling theater-range, nuclear-capable platforms by providing means for disabling or otherwise interfering with their guidance, communications, or other key internal systems.[72]

Another challenge is that US platforms will likely be operating within a contested, high-risk environment and may be searching for a moving target accompanied by conventional forces. These cases may require locally generated, high-penetration, precise engagement options that are highly discriminate and capable of striking both priority platforms and their defenses (such as theater-range, nuclear-capable delivery systems protected by air-defense batteries). Moreover, policy makers and combatant commanders will likely seek to minimize the risk to US personnel; if available, they will either employ unmanned systems or manned-unmanned combinations that reduce human exposure to hazardous environments. Emerging strike delivery options such as the Golden Horde and CLEAVER programs provide expendable, semiautonomous weapons that can significantly increase standoff strike capacity across a theater, granting US commanders numerous options for attacking an adversary's forces while keeping US forces out of harm's way.[73]

These and other examples of "smart" weapons currently fielded or under development could be important cost imposition tools for dealing with

CNI opponents. An additional benefit of these conventional systems is their complementary traits of rapid incorporation expandable across a coalition and slew of delivery platforms as well as, in relative terms, their low costs per unit or weapon.[74] By providing US forces with large numbers of inexpensive weapons that are dispersed across multiple bases and platforms and able to operate in a wide range of nonpermissive environments, these strike options can obviate some of the perceived benefits of intermingling forces and seriously complicate the planning of a CNI adversary. Even when its strike systems (conventional and nuclear-capable) are protected by active defenses or appear to be operating away from American strike platforms, these types of smart weapons will be able to hold all these forces—offensive and defensive—at risk of a sudden, accurate, lethal conventional attack.

Tailor communications. A threat that is not effectively communicated or fully understood is not credible, regardless of the military capabilities behind it. US policy makers should develop tailored strategic communications plans aimed at influencing the cost-benefit calculus of potential CNI opponents. Through public speeches and statements at events or engagements (particularly with allies and partners), policy makers should emphasize the risks potential adversaries face if they fail to disentangle their nuclear forces or choose to engage in theater nuclear brinkmanship. At the same time, however, they should also tout the potential benefits these states can realize through joining arms control talks, agreeing to implement confidence-building measures, and engaging in Track 1 and Track 2 dialogues. In turn, US combatant commanders, whose public statements are also closely watched by the capitals of both allies and potential adversaries, can broadcast these same messages to their defense counterparts across the region.

US policy makers should draw a clear distinction within their public messaging between a potential adversary's approach to CNI and the regional defense strategy and deterrence posture of the United States and its allies. Opening talking points could focus on potential adversaries' overreliance on destabilizing (and vulnerable) theater-range, nuclear-capable forces to attempt to hold US and allied forces within the region at risk. In contrast, the United States and its allies have a wide range of conventional ways and means for locating and either disabling or destroying an adversary's key theater-range strike systems (however armed) and, more broadly, for halting any combined conventional-nuclear theater offensive. Furthermore, the effectiveness of these conventional operations is enhanced by the enduring US commitment to extended deterrence. This provision of a

US "nuclear umbrella" is neither static nor applicable only in dire crises. It is an integral part of a broader US regional defense posture that includes conventional and nuclear-capable forces and is calibrated to meet contemporary security challenges, to include neutralizing adversary efforts to use nuclear threats to shape the battlespace or otherwise alter US and allied conventional operations. Neither the United States nor its allies rely on nuclear saber rattling to communicate resolve, nor do they require nuclear strikes to realize US and allied theater campaign objectives. Indeed, the potential employment of US nuclear forces, which will never target civilians, remains solely reserved for "extreme circumstances."[75]

A second important message for US policy makers to emphasize is that these actors stand alone, and their efforts to use nuclear weapons to intimidate regional states betray their isolation and comparative military weakness. In contrast, the US approach to regional deterrence and assurance, including extended deterrence, is part of a common, coordinated theater defense posture based on consultation and cooperation rather than bullying. Indeed, the unique challenges posed by a potential adversary's integrated forces and nuclear weapons ultimately bind the United States and its allies more closely together. As a result, coalition forces are well prepared for a full range of adversary threats, can maintain combat effectiveness in even the most challenging operating environments, and are fully equipped to counter conventional and nuclear-capable platforms in theater.

Finally, US policy makers can state that US alliance networks—and the extended deterrence guarantees undergirding these relationships—function to impose significant costs on adversaries in times of both competition and conflict. With coalition forces able to hold an opponent's integrated forces at risk regardless of when, where, and how they seek to leverage nuclear threats, theater-range, nuclear-capable forces are not credible tools of coercion or war fighting. As such, the substantial resources potential adversaries devote to developing, fielding, and maintaining theater-range, nuclear-capable forces and their accompanying nuclear weapons entail significant resource costs without offering any real benefits.

Encourage Restraint

The third pillar of US deterrence strategies is encouraging restraint. As stated in *Deterrence Operations*, "Encouraging adversary restraint is the way in which US actions can influence adversary decision-makers' perceptions of the benefits and costs of not taking an action we seek to deter. Thus, encouraging adversary restraint involves convincing adversary decision-

makers that not undertaking the action we seek to deter will result in an outcome acceptable to them (though not necessarily desired by them)."[76]

Regarding the challenges posed by CNI, the United States should encourage adversaries to either halt or roll back their integration of conventional and nuclear-capable forces. A closely related objective is attempting to convince a potential adversary to convert its theater-range, nuclear-capable systems so that they can only deliver conventional munitions and making this nonnuclear status permanent and readily observable.[77] Overall, the United States seeks to convince potential adversaries that casting a nuclear shadow over a region is a costly, counterproductive endeavor not worth pursuing.

Deterrence Operations also indicates that encouraging restraint requires convincing a potential adversary there are viable alternatives to pathways the United States does not wish them to pursue (and that accepting this alternative will result in an outcome amenable to both). On some issues, this may entail finding a "minimax" solution whereby the United States and the other party reach a mutually advantageous agreement (and avoid a mutually costly outcome) despite their broader competition.[78]

Persuading a potential adversary to either roll back its integration of conventional and nuclear forces or give up some of the latter may require a combined diplomatic-military approach akin to the "dual track" employed by the United States and NATO prior to the negotiation of the 1987 Intermediate-Range Nuclear Forces (INF) Treaty. To counter the threat posed by new Soviet intermediate-range nuclear forces in the form of the SS-20 Pioneer missile, the United States developed its own highly capable intermediate-range, nuclear-capable platforms (which several NATO states then agreed to host). The United States, however, also offered a diplomatic "track" to Moscow, proposing arms control talks to potentially limit these types of forces. The Soviet Union, which viewed the United States' ground-launched intermediate-range missiles as particularly dangerous (due in part to fears they could spearhead a "decapitation" strike on its leadership) and increasingly concerned about the costs of a prolonged arms race, eventually agreed to a treaty eliminating both sides' arsenals of these types of theater-range delivery systems.[79]

A contemporary dual-track approach could focus the military track on the United States fielding its own type(s) of ground-launched, intermediate-range missiles previously banned by the INF Treaty; continuing to develop several types of locally generated, high-penetration, precise-engagement "smart" weapons such as those discussed above; increasing troop rotations, force levels, or pre-positioned equipment to areas

or allies subject to specific regional nuclear threats; or perhaps employing some combination of the above. At the same time as it took these steps boosting its ability to hold a potential adversary's theater-range, nuclear-capable platforms at risk, the United States could also offer diplomatic negotiations to limit these types of capabilities and their associated nuclear weapons. One possible approach could be the pursuit of an agreement representing a hybrid of nuclear and conventional arms control treaties, such as combining elements of the Conventional Forces in Europe (CFE) Treaty, INF Treaty, and New START. The agreement would provide for numerical limitations of certain types of weapon systems and inspections within a specific theater and verification measures confirming the nuclear or nonnuclear status of dual-capable platforms.

The success of these or other types of talks seeking to address CNI-related challenges will ultimately depend on a broad range of factors. Whether via arms control negotiations or the use of other ways and means to encourage restraint (such as sanctions designed to penalize the development of certain types of weapons), US policy makers can negotiate or operate from a position of strength when backed by flexible, effective military capabilities and strong support from allies. This position can pave the way for potential adversaries to accept restraint regarding nuclear integration or the deployment of theater-range, nuclear-capable forces.

Conclusion

Potential adversaries such as Russia, China, and North Korea are continuing to invest in theater-range, nuclear-capable delivery systems and the production of new nuclear warheads. Their integration of nuclear and conventional forces, to include for the purpose of theater campaign planning, is a present and future challenge for US policy makers and combatant commanders.

Deterring and countering CNI threats from potential adversaries requires an integrated, but not mirror-imaged, US response. Policy makers should clearly communicate that the US approach to CNI allows its forces to hold opposing high-value theater assets, such as theater-range, nuclear-capable forces, at risk throughout a conflict. Such a message credibly threatens defeat of their integrated forces with US conventional capabilities—all without ever resorting to bellicose threats of nuclear use. Moreover, when properly equipped, US combatant commanders will possess an uninterrupted alliance all-domain kill chain that can effectively isolate an adversary's nuclear assets and eliminate theater employment options.

By coupling cost imposition and deterrence by denial strategies, the United States can make clear to both adversaries and allies that attempting to introduce nuclear weapons into a regional military conflict will not provide the former with a pathway to victory. In addition, developing effective US strategies for negating the perceived benefits of CNI will strengthen the ability of policy makers to encourage potential adversaries to refrain from their dangerous reliance on theater-range, nuclear-capable forces and regional nuclear coercion. In the long term, these strategies may also contribute to broader efforts to encourage these actors to retire or negotiate away nuclear weapons and nuclear-capable platforms either designed or assigned for regional conflict. SSQ

Justin Anderson

Dr. Anderson is a senior policy fellow at the Center for the Study of Weapons of Mass Destruction at National Defense University. He earned an MA and a PhD in war studies at King's College London and a BA in diplomacy and world affairs at Occidental College.

Lt Col James R. McCue, USAF

Colonel McCue serves as a nuclear strategist at the Defense Threat Reduction Agency. He is an Air Force helicopter pilot with over 2,500 hours in various missions, including combat rescue and nuclear security. He is a graduate of the Air Force Institute of Technology's Nuclear Weapons Effects, Policy, and Planning course; Missouri State University's Defense and Strategic Studies program; and the National Defense University Counter-WMD Fellowship Program.

Notes

1. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, D.C.: DOD, 2018), 2, https://dod.defense.gov/.

2. The authors use the term "theater-range, nuclear-capable delivery systems" to refer to any platform (short-, medium-, or intermediate-range) that can affect the battlefield or operational depth of a given regional conflict.

3. As stated by a 2020 Congressional Research Service (CRS) report, "Recent missile tests suggest that North Korea is striving to build a credible nuclear warfighting capability designed to evade regional ballistic missile defenses." Mary Beth D. Nikitin and Samuel D. Ryder, "North Korea's Nuclear Weapons and Missile Programs," CRS In Focus report (Washington, D.C.: Congressional Research Service, July 2020), 1, https://fas.org/. See also Defense Intelligence Agency (DIA), *Global Nuclear Landscape 2018* (Washington, D.C.: DIA, 2018), 19–21, https://dod.defense.gov/; and Department of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea 2017: Report to Congress* (Washington, D.C.: DOD, 2018), 1, 4. For Russia's integration of "non-strategic" nuclear forces across the "full spectrum of conflict," to include regional or "limited" war-fighting strategies, see Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, D.C.: DIA, 2017), 22, 25, 32, https://www.dia.mil/. See also Dave Johnson, *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*, Livermore

Papers on Global Security No. 3 (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2018), 66–72, https://cgsr.llnl.gov/.

4. Brad Roberts, *On Theories of Victory, Red and Blue*, Livermore Papers on Global Security No. 7 (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2018), 23, https://cgsr.llnl.gov/.

5. Brad Roberts, *Living with a Nuclear-Arming North Korea: Deterrence Decisions in a Deteriorating Threat Environment* (Washington, D.C.: Stimson Center, November 2020), 7, https://www.stimson.org/.

6. Keith B. Payne, "Nuclear Deterrence in a New Age," *Comparative Strategy* 37, no. 1 (2018): 4, https://doi.org/10.1080/01495933.2018.1419708.

7. Thomas Schelling, *Arms and Influence* (Fredericksburg, VA: Bookcrafter's, 1966), 114; Sean Maloney, "Remembering Soviet Nuclear Risks," *Survival* 57 no. 4 (August/September 2015): 78–80, https://doi.org/10.1080/00396338.2015.1068558; and William Drozdiak, "Kohl Defends Missiles," *Washington Post*, 22 November 1983, https://www.washingtonpost.com/.

8. Paul Schulte, "Tactical Nuclear Weapons in NATO and Beyond: A Historical and Thematic Examination," 16–25, in *Tactical Nuclear Weapons in NATO*, eds. Tom Nichols, Douglas Stuart, and Jeffrey D. McCausland (Carlisle, PA: U.S. Army Strategic Studies Institute, 2012), 13–74, https://publications.armywarcollege.edu/.

9. The *2018 Nuclear Posture Review* made it imperative that the United States develop, in close coordination with its allies, an approach to counter the CNI threat. See Department of Defense, *2018 Nuclear Posture Review* (Washington, D.C.: DOD, 2018), VIII, https://media.defense.gov/.

10. James M. Acton, "Why Is Entanglement So Dangerous?" Carnegie Q&A, 23 January 2019, https://carnegieendowment.org/.

11. James Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99, https://www.mitpressjournals.org/; Thomas G. Mahnken and Gillian Evans, "Ambiguity, Risk, and Great Power Conflict," *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 57–77, https://www.airuniversity.af.edu/; Caitlin Talmadge, "Would China Go Nuclear?: Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (Spring 2017): 50–92, https://doi.org/10.1162/ISEC_a_00274; and Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (Autumn 2020): 91–109, http://dx.doi.org/10.26153/tsw/10220.

12. Mansoor Ahmed, "Pakistan's Tactical Nuclear Weapons and Their Impact on Stability," *Carnegie Regional Insight*, 30 June 2016, https://carnegieendowment.org/.

13. Alexei Arbatov, "A Russian Perspective on the Challenge of U.S., NATO, and Russian Non-strategic Nuclear Weapons," 152–162, in *Reducing Nuclear Risks in Europe*, eds. Steve Andreason and Isabelle Williams (Washington, D.C.: Nuclear Threat Initiative, 2011), 152–71, https://media.nti.org/.

14. Office of the Director of National Intelligence, "Director of Intelligence Daniel Coats on Russia's Intermediate-range Nuclear Forces (INF) Treaty Violation," press statement, 30 November 2018, https://www.dni.gov/.

15. DIA, *Global Nuclear Landscape*, 8.

16. Statement by Admiral Harry B. Harris, U.S. Navy, Commander, U.S. Indo-Pacific Command, House Armed Services Committee Meeting on U.S. Pacific Command Posture, 26 April 2017, https://docs.house.gov/.

17. David C. Logan, "Making Sense of China's Missile Forces," 401–8, in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, eds. Phillip Saunders et al. (Washington, D.C.: NDU Press, 2019), 393–435, https://ndupress.ndu.edu/.

18. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020* (Washington, D.C.: DOD, 2020), viii, https://media.defense.gov/; and Liu Xuanzun, "PLA Rocket Force Launches DF-26 'Aircraft Carrier Killer' Missile in Fast Reaction Drills," *Global Times* (China), 6 August 2020, https://www.globaltimes.cn/.

19. Ankit Panda, "North Korea Shows Increased Operational Confidence in Hwasong-12 IRBM," *The Diplomat*, 17 September 2017, https://thediplomat.com/; and Michael Elleman, "North Korea's Hwasong-12 Launch: A Disturbing Development," *38 North*, 30 August 2017, https://www.38north.org/.

20. DIA, *Global Nuclear Landscape*, 11, 22; and Rebeccah L. Heinrichs, "The Arms Control Landscape ft. DIA Lt. Gen. Robert P. Ashley, Jr.," event transcript, Hudson Institute, 31 May 2019, https://www.hudson.org/.

21. Henry Foy, "Russia Makes Missile Offer in Effort to Restart Talks on Arms Control," *Financial Times*, 26 October 2020, https://www.ft.com/.

22. David Logan, "Are They Reading Schelling in Beijing?: The Dimensions, Drivers, and Risks of Nuclear-Conventional Entanglement in China," *Journal of Strategic Studies* (2020): 19–24, https://doi.org/10.1080/01402390.2020.1844671.

23. Logan, 23.

24. Acton, *Escalation through Entanglement*, 59.

25. United Nations, Report of the Panel of Experts established pursuant to resolution 1874 (2009), 31 July 2019, S/2019/691, 135, https://www.securitycouncilreport.org/.

26. NATO, *The Secretary General's Annual Report 2015* (Brussels: NATO, 2015), 21; and Dave Johnson, "ZAPAD 2017 and Euro-Atlantic Security," *NATO Review*, 14 December 2017, https://www.nato.int/.

27. Xuanzun, "PLA Rocket Force Launches DF-26."

28. CGTN, "China's Rocket Force Launches New Missiles in Northwest China's Desert," YouTube video, 1:13, 29 January 2019, https://www.youtube.com/; CGTN, "PLA Rocket Force Brigade Holds Night Combat Drill," YouTube video, 1:00, 18 April 2018, https://www.youtube.com/; and CGTN, "China's 'Rocket Force' Conducts First Drill of New Year," YouTube video, 1:28, 3 January 2016, https://www.youtube.com/. See also CCTV, "Chinese Rocket Force Conducts Missile Launch Drills," YouTube video, 0:48, 11 June 2017, https://www.youtube.com/.

29. Anna Fifield, "North Korea Says It Was Practicing to Hit U.S. Military Bases in Japan with Missiles," *Washington Post*, 6 March 2017, https://www.washingtonpost.com/.

30. Kim Min-Seok, "The State of the North Korean Military," 21–23, in *Korea Net Assessment*, Chung Min Lee and Kathryn Botto, eds. (Washington, D.C.: Carnegie Endowment for International Peace, 2020), 19–30; and Department of Defense, *2019 Missile Defense Review* (Washington, D.C.: DOD, 2019), v, https://www.defense.gov/.

31. Min-Seok, 21–23; DOD, v; and Vince Manzo and John Warden, "Want to Avoid Nuclear War? Reject Mutual Vulnerability with North Korea," *War on the Rocks*, 29 August 2017, https://warontherocks.com/.

32. Brad Roberts, "Strategic Competition in the 21st Century: Theories of Victory, Red and Blue," presentation, Lawrence Livermore Center for Global Security Research, YouTube video, 50:08, 21 May 2015, https://www.youtube.com/.

33. George F. Kennan's "Long Telegram" assessment of the Soviet Union provides observations that can also apply to contemporary autocratic states, to include that they cannot accept a lasting peace or conclusion of competition with the United States and its democratic allies; any "peace" or acceptance of a stable relationship is tactical and temporary. Wilson Center Digital Archive, "George Kennan's 'Long Telegram,'" 22 February 1946, https://digitalarchive.wilsoncenter.org/.

34. National Intelligence Council (NIC), "Russia and Eurasia," in *Global Trends: Paradox of Progress* (Washington, D.C.: NIC, 2017), 125, https://apps.dtic.mil/dtic/; Michael Mazarr, "The Essence of Strategic Competition with China," *PRISM* 9, no. 1 (2020): 3–22, https://ndupress.ndu.edu/; and Richard Javad Heydarian, "China's Premature Bid for Hegemony in Southeast Asia," *Order from Chaos* (blog), Brookings, 28 November 2018, https://www.brookings.edu/.

35. Stephan Evans, "The Saddam Factor in North Korea's Nuclear Strategy," *BBC News*, 9 September 2016, https://www.bbc.com/; and James C. Mulvenon et al., *Chinese Responses to U.S Military Transformation and Implications for the Department of Defense* (Washington, D.C.: RAND Corporation, 2006), 10.

36. Vince Manzo and John Warden note that "an adversary of the United States and its allies may believe it can conduct limited nuclear strikes and, rather than precipitate its own destruction, win the war—not in the sense of defeating the United States military, but by convincing Washington to refrain from bringing its full strategic-military power to bear on the conflict." See Vince Manzo and John Warden, "After Nuclear First Use, What?" *Survival* 60, no. 3 (February 1980): 133–60, https://doi.org/10.1080/01495933.2020.1702341.

37. Jung Pak, "What Kim Wants: The Hopes and Fears of North Korea's Dictator," *Foreign Affairs*, May/June 2020, https://www.foreignaffairs.com/.

38. The *2014 Quadrennial Defense Review* recognized this challenge, stating that the United States (and its nuclear forces) will ensure "potential nuclear-armed adversaries that they cannot escalate their way out of failed conventional aggression." Department of Defense, *2014 Quadrennial Defense Review* (Washington, D.C.: DOD, March 2014), 13, http://archive.defense.gov/.

39. DOD, *2018 Nuclear Posture Review*, 14.

40. Bernard Brodie, *Escalation and the Nuclear Option* (Santa Monica, CA: RAND Corporation, 1965), vi, https://www.rand.org/.

41. Kevin Ryan, "Is 'Escalate to De-escalate' Part of Russia's Nuclear Tool Box?," Russia Matters, Harvard Belfer Center, 8 January 2020, https://www.russiamatters.org/.

42. "Russia Threatens to Aim Nuclear Missiles at Denmark Ships if it Joins NATO Shield," Reuters, 22 March 2015, https://www.reuters.com/; and " 'Norway Will Suffer': Russia Makes Nuclear Threat over US Marines," *The Local*, 31 October 2016, https://www.thelocal.no/.

43. Jack Kim and Kiyoshi Takenaka, "North Korea Threatens to 'Sink' Japan, Reduce US to 'Ashes and Darkness,'" Reuters, 14 September 2017, https://www.reuters.com/; and "North Korea Threatens US and S. Korea with Nuclear Strikes," *BBC News*, 7 March 2016, https://www.bbc.com/.

44. The quote is attributed to French president Charles De Gaulle, whose answer was a definitive "non," leading France to develop its nuclear force de frappe. Drew

Middleton, "The De Gaulle Nuclear Doctrine Is Alive in Paris," *New York Times*, 6 May 1981, A16, https://www.nytimes.com/. See also Jamie Shea, "1979: The Soviet Union Deploys Its SS20 Missiles and NATO Responds," NATO video lecture, 4 March 2009, https://www.nato.int/.

45. Michael Kofman, Anya Fink, and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts* (Washington, D.C.: Center for Naval Analyses, April 2020), 12, https://www.cna.org/.

46. Christian Lowe, "Russia Defends Right to Deploy Missiles after Kaliningrad Rebuke," Reuters, 6 February 2018, https://www.reuters.com/.

47. This allied fear of "decoupling," which was also present during the Cold War, has returned but now applies to the potential threat posed by more than one actor. See Yochi Dreazan, "Here's What War with North Korea Would Look Like," *Vox*, 8 February 2018, https://www.vox.com/; and Mira Rapp-Hooper, "Decoupling Is Back in Asia: A 1960s Playbook Won't Solve These Problems," *War on the Rocks*, 7 September 2017, https://warontherocks.com/.

48. This is a "deterrence by doubt" defense. "Interview: Lt. Gen. Raad Al-Hamdani," *Frontline*, PBS, 26 February 2004, http://www.pbs.org/.

49. James Acton, "Inadvertent Escalation and the Entanglement of Nuclear Command-and-Control Capabilities," Belfer Center Policy Brief, 29 October 2018, https://www.belfercenter.org/.

50. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook 2020* (Washington, D.C.: Department of Defense, 2020), 224, https://fas.org/.

51. Alexei Arbatov, "A Russian Perspective on the Challenge of US, NATO, and Russian Non-strategic Nuclear Weapons," 152–71, in *Reducing Nuclear Risks in Europe: A Framework for Action*, eds. Steve Andreasen and Isabelle Williams (Washington, D.C.: Nuclear Threat Initiative, 2011): 162–63, https://media.nti.org/.

52. Col Kenneth P. Ekmen, "Applying Cost Imposition Strategies against China," *Strategic Studies Quarterly* 9, no. 1 (Spring 2015): 26, 30, https://www.airuniversity.af.edu/.

53. Department of Defense, *Deterrence Operations – Joint Operating Concept*, ver. 2.0 (Washington, D.C.: DOD, December 2006), 5, https://www.jcs.mil/.

54. Department of Defense, *2018 Nuclear Posture Review*, VIII.

55. David Santoro and Robert Gromoll, *On the Value of Nuclear Dialogue with China* (Honolulu, HI: Pacific Forum, 2020): 8–9, https://pacforum.org/; Brad Roberts, "Strategic Stability Under Obama and Trump," *Survival* 59, no. 4 (2017): 57, https://doi.org/10.1080/00396338.2017.1349780; Nuclear Threat Initiative (NTI), "Russia Rejects Immediate Talks on Tactical Nuke Cuts," 8 February 2011, https://www.nti.org/; Radio Free Europe/Radio Liberty, "Russia Sees 'No Prospects' for Extending Nuclear Pact with U.S.," 14 October 2020, https://www.rferl.org/; "Russia Suspends Joint Consultations on Treaty on Conventional Armed Forces in Europe," TASS, 10 March 2015, https://tass.com/russia/781973; Julia Masterson and Kelsey Davenport, "North Korea Rejects U.S. Proposal," *Arms Control Now* (blog), Arms Control Association, 10 October 2019, https://www.armscontrol.org/; and Duyeon Kim, "N. Korea Launches Rocket, Kills U.S. Deal," *Arms Control Today*, Arms Control Association, 8 May 2012, https://www.armscontrol.org/.

56. S. T. Belyaev et al., "The Black Sea Experiment: The Use of Helicopter-Borne Neutron Detectors to Detect Nuclear Warheads in the USSR-US Black Sea Experiment," *Science and Global Security* 17, nos. 2-3 (2009): 186–93, http://scienceandglobalsecurity.org/.

57. Richard Maurer et al., "Aerial Neutron Detection: Neutron Sensors for Nonproliferation and Emergency Response Applications," National Security Technologies, Report DOE/NV/25946-1634, October 2012, 48, https://doi.org/10.2172/1136549. In more recent years, experiments conducted around the Fukushima Daiichi Nuclear Power Plant destroyed by the tsunami that struck Japan in 2011 have demonstrated that unmanned drones can detect localized radiation sources and hotspots from 150 to 300 meters. Jiang et al., "A Prototype of Aerial Radiation Monitoring System Using an Unmanned Helicopter Mounting a GAGG Scintillator Compton Camera," *Journal of Nuclear Science and Technology* 53, no. 7 (2016): 1067–75, published online 5 October 2015, https://doi.org/10.1080/00223131.2015.1089796.

58. Gabriel Almodovar et al., "Joint Integrated Air and Missile Defense: Simplifying an Increasingly Complex Problem," *Joint Force Quarterly* 88 (1st Qtr 2018): 78–84, https://ndupress.ndu.edu/.

59. Joint Publication 3-01, *Countering Air and Missile Threats*, 21 April 2017 (validated 2 May 2018), https://www.jcs.mil/.

60. For example, the United States developed plans for a theater missile defense exercise with Japan and South Korea shortly after North Korea conducted its November 2017 test of the Hwasong-15 missile. Ankit Panda, "US, Japan, South Korea to Hold Missile Tracking Exercise," *The Diplomat*, 11 December 2017, https://thediplomat.com/.

61. Office of the Secretary of Defense, *2019 Missile Defense Review* (Washington, D.C.: Department of Defense, 2019), https://www.defense.gov/; US Army, *Army Air and Missile Defense Vision 2028* (Huntsville, AL: USASMDC/ARSTRAT, March 2019), https://www.smdc.army.mil/; and Kenneth R. Dorner, William B. Hartman, and Jason M. Teague, "Back to the Future: Integrated Air and Missile Defense in the Pacific," *Air and Space Power Journal* 29, no. 1 (January-February 2015): 61–78, https://www.airuniversity.af.edu/.

62. Joseph Trevithick, "F-35 Cueing Artillery to Take Out Air Defense Site Is a Glimpse of the Future," *The Drive*, 13 December 2019, https://www.thedrive.com/.

63. "Passive defenses" broadly refer to static defenses and techniques such as dispersal of forces, inasmuch as the latter involves movement before or during conflict.

64. US Army News Service, "US Army Corps of Engineers, Far East District, Completes Construction of Third Generation of Hardened Aircraft Shelters at Kunsan Air Base," 27 May 2020, https://www.army.mil/.

65. Jaganath Sankaran, " 'Big, Fat, Juicy Targets'—The Problem with Existing Early-Warning Satellites. And a Solution," *Bulletin of Atomic Scientists*, 30 September 2019, https://thebulletin.org/.

66. George I. Seffers, "Air Force Seeks Disaggregated Command and Control," *Signal*, 1 February 2019, https://www.afcea.org/.

67. Hailey Haux, "A B-52 Exercises Dynamic Force Employment with Joint Partners in Indo-Pacific," Pacific Air Forces Public Affairs press release, 7 July 2020, https://www.pacom.mil/.

68. Charles A. Salter, "Psychological Effects of Nuclear and Radiological Warfare," *Military Medicine* 166, Suppl. 2 (2001): 17–18.

69. Following a series of exercises in which most personnel wore personal protective equipment for most of the activity, a November 2019 US Army 1st Armored Division report noted, "Much of what will be asked of a Soldier against a near-peer threat in a contaminated battlefield will require fighting 'dirty' for extended periods of time. Maneuver formations at the brigade level and lower will need to conduct hasty decontamination as far forward as possible to continue to sustain operational tempo." Kurt Ebaugh, "News from the CTC: Unit CBRN Readiness Training – A Way," Center for Army Lessons Learned, November 2019, https://usacac.army.mil/.

70. DOD, *Deterrence Operations – Joint Operating Concept*, 26–27.

71. Nonexplosive Hellfire missiles have a proven combat record eliminating high-value targets on the move with exceptionally low collateral risk. See Gordan Lubold and Warren P. Strobel, "Secret Missile Targets Terrorist Leaders," *Wall Street Journal*, 10 May 2019, A4.

72. One example of such a system would be Boeing's Counter-electronics High Power Microwave Advanced Missile Project (CHAMP), a "non-kinetic, non-lethal" weapon first tested in 2012 that uses "bursts of high-powered energy" to destroy electronics systems and microchips, "effectively knocking out a specific target's data and electronic subsystems" and rendering it inoperable. "CHAMP – Lights Out," Boeing press release, 22 October 2012, https://www.boeing.com/; and George I. Seffers, "CHAMP Prepares for Future Flights," *SIGNAL*, 1 February 2016, https://www.afcea.org/. Similarly, other electronic attack systems may be able to directly disable delivery systems by interfering with internal or external systems or networks that enable them to conduct attacks. Brendan I. Koerner, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *Wired*, 18 February 2014, https://www.wired.com/; and Joseph Trevithick, "Navy to Add Laser Weapons to at Least Seven More Ships in the Next Three Years," *The Drive*, 8 July 2020, https://www.thedrive.com/.

73. The "Golden Horde" is a US Air Force "Vanguard program" that, via an innovative combination of hardware and software, can provide aircraft with "munitions [that] can be networked together and operate autonomously after launch according to a set of predetermined rules." Valerie Insinna, "US Air Force Gears Up for First Flight Test of Golden Horde Munition Swarms," *Defense News*, 13 July 2020, https://www.defensenews.com/. Golden Horde, after being fired by a pilot, can split up to strike both the intended target (e.g., air defense systems) and other, higher-priority targets (e.g., mobile missiles leaving hide sites) that are not identified until after the weapons are inbound. The Cargo Launch Expendable Air Vehicle with Extended Range (CLEAVER) system is designed to allow cargo planes to drop multiple "palletized munitions" that contain "long-range, high precision weapons [that can] destroy moving and non-moving targets." Whitney Wetsig, "AFRL, AFSOC Launch Palletized Weapons from Cargo Plane," *Air Force News*, 28 May 2020, https://www.af.mil/.

74. Weapons such as the CLEAVER, dropped from standard cargo planes, can provide strike options that are significantly less expensive than medium- or long-range bombers. This is especially true for offering such technology to partners and allies in an attempt to cheaply attain dispersion and redundancy of long-range precision-strike capabilities.

75. DOD, *2019 Nuclear Posture Review*, II.

76. DOD, *Deterrence Operations – Joint Operating Concept*, 27.

77. Under the terms of START, for example, the United States agreed to convert its dual-capable B-1B bombers to conventional-only platforms. A "metal cylindrical sleeve

was welded into the aft attachment points," making it impossible for the aircraft to carry nuclear-armed cruise missiles from its wings, and cable connectors required to arm nuclear weapons were also removed. US Air Force, "B-1 Bomber," fact sheet, 16 December 2015, https://www.af.mil/.

78. Thomas C. Schelling, "The Strategy of Conflict: Prospectus for a Reorientation of Game Theory," *Journal of Conflict Resolution* 2, no. 3 (September 1958): 209–19, https://doi.org/10.1177/002200275800200301.

79. Louis Sell, *From Washington to Moscow: US-Soviet Relations and the Collapse of the USSR* (Durham, NC: Duke University Press, 2016), 204.

Corporate Hackers: Outsourcing US Cyber Capabilities

Charles W. Mahoney

Abstract

Cyberspace is a key war-fighting domain that affects all aspects of United States national security. Although defense contractors are essential to United States cyber operations, little research has examined the specific cyber services military and intelligence agencies outsource to corporations. This article evaluates government contracting practices in three strategically important United States cyber markets: cybersecurity, offensive cyber operations, and data analytics. Each market possesses distinct structural economic features that affect cyber outsourcing. After almost two decades of contracting, the cybersecurity market functions efficiently because it is competitive and information about the capabilities of corporate suppliers is widely available. Conversely, the small number of suppliers in the offensive cyber market coupled with the limited commercial utility of offensive cyber tools suggests that the sector may develop into an oligopoly in which the United States government is highly dependent on contractors. Finally, data analytics is a relatively new field comprised of numerous corporate suppliers that possess limited experience working with the Department of Defense and the intelligence community. Lack of information about companies' relative capabilities in the data analytics market means that government agencies are likely to make suboptimal contracting decisions when choosing among prospective suppliers.

*****

Cyberspace is a key war-fighting domain that affects all aspects of United States national security.[1] Although defense contractors are essential to United States cyber operations, little research has examined the specific cyber services military and intelligence agencies outsource to corporations.[2] Furthermore, the nature of contracting between government agencies and corporate cyber service providers remains understudied.[3] What types of cyber operations do defense contractors carry out for United States military and intelligence agencies? Is United States cyber outsourcing efficient? That is, do government agencies accurately identify the most qualified cyber service providers, capably monitor their

behavior, and foster competitive markets that encourage innovation while keeping costs affordable?

This article argues that structural economic differences in three distinct cyber markets—cybersecurity, offensive cyber operations, and data analytics—have important implications for the quality of outsourcing carried out by United States defense and intelligence agencies. In the cybersecurity market, which has existed for over 20 years, contracting is relatively efficient. The market is characterized by numerous suppliers, and government agencies possess detailed information about corporations' capabilities and past performances. By contrast, the emerging market for offensive cyber operations has a small number of suppliers, and the tools companies develop for offensive cyber missions have limited utility outside national security settings. These two factors are likely to lead to an inefficient market in which government agencies are highly dependent on contractors. Finally, the market for "big data" analytics—which involve collection, analysis, and visualization of information using algorithms—is relatively new. Thus, the Department of Defense (DOD) and intelligence community have little experience assessing the capabilities of competing firms. This feature of the analytics market means that government agencies are more likely to make suboptimal choices when assessing the relative capabilities of companies in the field. However, the competitive nature of the analytics market coupled with the wide applicability of analytics products outside defense-specific settings suggests that assessment and oversight of firms will become more efficient as information about companies increases through repeated contracting.

This article first describes three key United States defense markets for cyber operations and identifies the major companies active in each market. Next, it presents concepts from transaction cost economics and applies this body of theory to government outsourcing in the cybersecurity, offensive cyber, and data analytics markets. The article then examines two important cases of United States government cyber contracting: The Department of Homeland Security's $1 billion Development, Operations, and Maintenance (DOMino) contract and the United States Army's $876 million Distributed Common Ground System A-2 (DCGS-A2) contract. The conclusion summarizes major findings and presents policy recommendations for future military and intelligence cyber outsourcing.

Defense Contracting and United States Cyber Operations

American military and intelligence agencies have an extensive history of procuring goods and services from corporations.[4] By outsourcing non-

essential duties and hardware production to contractors, the national security community can more efficiently focus on its core strategic planning and war-fighting responsibilities. Additionally, companies are an important source of technological innovation for the armed forces.[5] Although partnership with the private sector is a key pillar of American national defense, in recent decades the government has increasingly outsourced vital national security functions historically carried out by Soldiers and civilian government employees.[6] As a recent Congressional Research Service report notes, "without contractor support, the United States would not be able to arm and field an effective fighting force."[7]

Cyber operations are an emerging field in which the DOD and the intelligence community are highly integrated with the private sector and where contractors perform mission critical functions. In 2017, the United States government authorized $19.8 billion in unclassified spending for all cyber related activities performed by defense contractors, an increase of 120 percent over 2012 levels.[8] Scholars have advanced several typologies to classify varying types of cyber operations. While academic debate in this area is likely to persist, there is emerging consensus that distinct differences exist among cybersecurity—which includes defensive cyber operations,[9] offensive cyber operations, and data analytics.[10] What follows is an analysis of outsourcing in these three strategically important cyber markets.

Cybersecurity

The Joint Chiefs of Staff define *cybersecurity* as activities that protect United States government data, networks, and cyberspace-enabled hardware by defeating malicious cyber activity carried out by adversaries.[11] Various technical responsibilities fall within the broad category of cybersecurity, including providing network defense, software application security, protection of command and tactical communications, and hardware and infrastructure protection against electronic attacks. The central objectives of cybersecurity operations are to protect United States government computers and electronic communication systems and to ensure that military and intelligence agencies possess data availability, integrity, and confidentiality.[12]

Among the three main categories of cyber operations, cybersecurity comprises the largest share of federal government spending, accounting for 75 percent of funds spent on all outsourced cyber activities related to national defense between 2012 and 2017.[13] The corporations receiving the bulk of defense-related funding for cybersecurity operations during this period include Northrop Grumman, Lockheed Martin, Perspecta, IBM,

Dell, General Dynamics, Leidos, Booz Allen Hamilton, Raytheon, CACI, and SAIC.[14] These companies provide "full spectrum" cybersecurity capabilities. That is, they offer government agencies a suite of services ranging from network risk analysis and cyber threat anticipation through cyber incident response and digital forensics. For example, Booz Allen Hamilton uses "cyber fusion centers" to support the DOD and intelligence community with services including vulnerability assessment, threat prevention, red team testing, and cyberattack detection and response.[15] Similarly, Leidos offers full-spectrum cyber services using a "security operations center" approach that supports government agencies by detecting, managing, and responding to cyber threats. The largest corporations providing the federal government with cybersecurity services employ thousands of specialists whose skills are in high demand. General Dynamics alone employs over 3,000 cyber professionals who work with government agencies in an effort to improve the nation's defensive cyber capabilities.[16] By comparison, the United States Cyber Command (CYBERCOM)—the DOD's organizational hub for coordinating the military's cyber operations—presently has approximately 1,000 full-time military and civilian staff members.[17]

A notable feature of the cybersecurity market is the recent entrance of prime defense contractors, traditionally associated with hardware production, into the sector. In part, prime contractors' shift into cybersecurity has occurred out of necessity. As hardware becomes increasingly integrated with applications that run in cyberspace, corporations must ensure that the satellite systems, planes, drones, and tanks they produce are "cyber resilient" against enemy attack. However, many major contractors—including Raytheon, Northrop Grumman, and Lockheed Martin—have also begun providing government agencies with cybersecurity services not directly associated with the hardware they design and build. Raytheon, for example, supplies cybersecurity services to the Department of Homeland Security and other government agencies as part of the $1 billion DOMino contract.[18] Northrop Grumman, another major manufacturer of military hardware, recently won an Air Force contract to provide CYBERCOM with rapid access to a "full spectrum of cyber capabilities."[19]

Another significant trend in cybersecurity operations is the emergence of major commercial technology companies as suppliers to the national security community. In the past, technology firms often were reluctant to work with the DOD and CIA for fear of damaging their brands. In recent years, however, Amazon, Microsoft, and Oracle have become direct competitors to traditional federal information technology (IT) contractors in certain cybersecurity service areas, particularly network and cloud

security.[20] In 2013, for example, Amazon won a $600 million contract to modernize the CIA's computer networks.[21] As part of this transition, Amazon was responsible for securing sensitive information stored and operated in its cloud platform. Amazon has publicly acknowledged that the defense industry represents a major focus of its future strategic business plans: "The defense, intelligence, and national security communities deserve access to the best technologies in the world[,] . . . and we [Amazon] are committed to supporting their critical missions."[22] Another high-profile example of commercial technology firms' rise in the cybersecurity market is the Pentagon's Joint Enterprise Defense Infrastructure (JEDI) project, a $10 billion contract that attracted proposals from Amazon, Microsoft, Google, IBM, and Oracle. The JEDI project tasks one company with managing the DOD's transition from traditional to cloud-based computer systems. A central part of this transition involves securing classified Pentagon information stored in cloud networks.[23] Microsoft was awarded the JEDI contract in 2019; however, Amazon is actively contesting the award.[24]

Offensive Cyber Operations

Cybersecurity operations protect United States government computer networks. By contrast, offensive cyber operations seek to penetrate enemy cyberspace and, at times, to impair adversaries' hardware and critical physical infrastructure.[25] The Joint Chiefs of Staff note that all cyber operations conducted outside of "blue cyberspace"—areas in cyberspace protected by the government and its mission partners—are classified as offensive cyber operations.[26] Therefore, causing kinetic damage is not a necessary criteria for a cyber operation to be considered offensive in nature. In fact, much offensive cyber activity carried out by the DOD and the intelligence community consists of efforts to gather intelligence, with no intent to cause immediate physical or functional damage to adversaries' computer systems or infrastructure. These types of nondestructive offensive cyber operations are referred to as "cyber exploitation" and constitute the primary activity of defense contractors operating in the offensive cyber market.

In 2017, federal spending on offensive cyber activities outsourced to contractors totaled $2.6 billion, an increase of 65 percent over 2016 outlays.[27] Contractors' offensive cyber activities include environment preparation and cyber tools development, which both involve penetration of adversaries' computer networks. Environment preparation consists of efforts to penetrate enemy cyberspace in order to evaluate the capabilities, intentions, and potential threats posed by adversaries.[28] Environment preparation can be considered surveillance and reconnaissance in cyberspace and

is key to the DOD's "defend forward" approach to cyber threats, which stresses halting malicious cyber activity at its source.[29] Cyber tools development entails creating code and applications that can be used to access and potentially damage enemy networks, hardware, and infrastructure. Defense contractors that support cyber tools development are often referred to as "offensive cyber operations planners" and assist the DOD and intelligence agencies in the design phase of offensive cyber missions. Although some contractors are increasingly willing to acknowledge that they take part in offensive cyber operations, most maintain that they neither build cyber weapons nor direct offensive cyber operations. According to company representatives, both of these activities remain the exclusive responsibility of the military and the intelligence community.[30]

Defense contractors active in the offensive cyber market include Northrop Grumman, Booz Allen Hamilton, ManTech International, CACI, General Dynamics, Leidos, Lockheed Martin, BAE Systems, and SAIC. The private sector market for offensive cyber is relatively new, and corporations doing business in the field have only recently publicly acknowledged their role in these operations.[31] Some companies now overtly advertise their offensive cyber capabilities. ManTech International, for instance, claims that its "offensive cyber experience is unrivaled within the Intelligence Community and Department of Defense" and that the company provides services including "vulnerability research" and "media and hardware exploitation."[32] CACI touts an "expert offensive cyber operations team" that provides support against "adversarial platforms."[33] In contrast to ManTech and CACI, SAIC is less overt about its offensive cyber work; however, the company frequently advertises job openings for "offensive cyber planners" on its website, and SAIC executives have acknowledged that the offensive cyber market is an important growth area for the company.[34]

From the vague language that corporations publicly use to describe their offensive cyber services, it is evident that this area of operations is highly classified and also represents a potential legal and public relations challenge for contractors. Because offensive cyber operations involve missions that infiltrate adversaries' cyberspace, they represent behavior that could be considered "inherently governmental"[35]—that is, duties that by United States law or policy must be performed by federal government employees.[36] In the Iraq War and the war in Afghanistan, several defense contractors—most notably Blackwater—were alleged to have engaged in activities that constituted inherently governmental functions.[37] Since that time, government agencies have sought to delineate clearly those activities that must remain

the responsibility of government personnel and those that contractors can perform. In kinetic domains, this has resulted in a clear distinction between Soldiers—whose responsibilities may entail physical violence or kill-chain decisions—and contractors, who are not permitted to directly take part in activity that may "significantly affect the life, liberty or property of private persons."[38] In the emerging domain of offensive cyber operations, the activities that constitute inherently governmental functions remain less clearly defined. This may pose a challenge in the future if contractors assist government agencies with cyber missions that result in casualties or significant damage to physical infrastructure.

Data Analytics and Machine Learning

The third major area of government spending on cyber capabilities is in the field of data analytics, which is closely related to machine learning and artificial intelligence. This emerging service area involves data mining, predictive algorithms, and visualization tools that can inform both kinetic and cyberspace missions.[39] Thus, while traditional cyber operations form part of the data analytics field, the potential applications of data analytics tools are extremely diverse. In the realm of cybersecurity, analytics applications use algorithms to gather information about cyber threats in order to identify and neutralize malicious code. Analytic cyber tools may also be offensive in nature, such as Russia's use of automated malware in recent cyberattacks against Ukraine.[40] Within the national security community, agencies are increasingly turning to machine-led data analysis to assist in mission critical decision-making.[41]

In 2017, the federal government spent $1.4 billion on services provided by contractors to enhance analytics and machine learning capabilities related to cyber operations.[42] These services include incident response and forensics, continuous diagnostics and mitigation, and data visualization.[43] Leading companies in this field include Palantir, KBR, Raytheon, Perspecta, and Booz Allen Hamilton.[44] The market for machine learning–supported cyber tools is dynamic and includes numerous start-up companies that supply a variety of different services. More so than other cyber markets, advances in machine learning technologies are taking place at corporations not considered pure-play defense contractors. This reality has altered traditional DOD methods of procurement and has caused established defense contractors to anticipate challenges from upstart firms. To gain a foothold in the data analytics market, many existing corporations in the defense industry have pursued strategic acquisitions.[45] For instance, in 2018 Perspecta—formerly the public-sector services division of DXC

Technology—acquired Vencore and Keypoint, two smaller firms specializing in machine learning and cybersecurity. With these acquisitions, Perspecta leveraged its existing relationships with the DOD and the intelligence community to rapidly become one of the leading cyber data analytics suppliers in the defense industry. Similarly, KBR—a company primarily known for its oil and gas logistics capabilities—acquired data analytics firm Stinger Ghaffarian Technologies (SGT) for $355 million in 2018. KBR now brands itself as a leader in big data, artificial intelligence, and machine learning and is focusing much of its future business on cyber operations in addition to its core energy services enterprise.

In contrast to Perspecta and KBR, data analytics firm Palantir has its roots in the Silicon Valley start-up community. Established in 2003 by a group of investors that included PayPal co-founder Peter Thiel, in its early years Palantir was supported by investments from CIA-backed venture capital organization In-Q-Tel.[46] In the wars in Iraq and Afghanistan, Palantir's software was used by both the CIA and Marine Corps to support counterterrorism missions.[47] Since the late 2000s, Palantir's analytic tools—which involve data mining, predictive algorithms, and data visualization—have been adopted by numerous defense and intelligence agencies as well as by private sector businesses.[48] Palantir's Gotham platform is used by the intelligence community to analyze "data sources, unstructured cable traffic, structured identity data, email, telephone records, spreadsheets, [and] network traffic" to inform intelligence analysis.[49] Similarly, Palantir's Phoenix and Hercules systems are used for cybersecurity by government agencies and the private sector and employ data mining and machine learning technologies to autonomously identify and mitigate cyber threats.[50] The company's rapid rise within the United States defense community has resulted in a corporate valuation of over $45 billion, and it is now a publicly traded corporation.[51]

Although data analytics and machine learning presently represent a small segment of the United States cyber services market, technological advances in the field have the potential to affect the global balance of power.[52] This prospect is supported by the substantial investment countries are making in artificial intelligence technologies. China, for instance, is a world leader in facial recognition capabilities and has identified artificial intelligence as an "existential priority."[53] Similarly, Russian president Vladimir Putin famously asserted that whatever state becomes dominant in artificial intelligence "will be the ruler of the world."[54] While machine learning has utility in traditional defensive and offensive cyber operations, its potential applicability to numerous other facets of military plan-

ning and operations—both in cyberspace and in physical domains—is broad. For this reason, the market for data analytics and machine learning services is perhaps the most lucrative and strategically important cyber sector going forward.

Transaction Cost Economics and Defense Contracting

This inquiry applies two related bodies of theory, transaction cost economics and principal-agent theory, to explain features of United States cyber outsourcing. Both areas of knowledge examine relationships in which a principal, often a corporation or government agency, enters into a contractual relationship with a second organization—the agent—tasked with providing a good or service to the principal in exchange for a fee. According to these theories, both corporations and government bureaucracies regularly procure goods and services from outside suppliers because they confront the "make or buy" decision.[55] That is, organizations must determine what goods and services they can efficiently produce internally and what inputs and operations are more efficiently supplied to them by the market via contracting.[56] In the context of defense outsourcing, this question can be reframed by asking, What services—excluding inherently governmental functions—are most effectively performed by Soldiers and government employees, and which are more efficiently supplied to the DOD and the intelligence community by the private sector?[57]

A central assumption in both principal-agent theory and transaction cost economics is that participants in any contractual agreement are limited by imperfect information. This bounded rationality signifies that all complex, long-term contracts are inherently incomplete and contain what economist Oliver Williamson refers to as "gaps, errors, and omissions" that may result in varying interpretations of a contract's meaning.[58] In business relationships governed by contracts, several potential inefficiencies—referred to as transaction costs—may result from imperfect contracts. For example, in the contract bidding phase, principals may make suboptimal decisions when choosing among potential suppliers. This "adverse selection" results from information asymmetries that exist between principals and agents with respect to the capabilities of companies competing for a contract award. In the execution phase of a contract, principals often face challenges assessing agents' performance.[59] Because principals usually cannot monitor the totality of agents' activities—and may even lack the expertise to effectively evaluate agents' output—they inevitably allot a degree of "agency slack" to contracted firms.[60] Finally, even if principals find that agents have shirked their obligations, it can be difficult for them to

enforce agreements because of the imprecise nature of contracts' language and the costs associated with finding an alternate supplier or seeking financial recompense in the courts.

An additional inefficiency that may arise in outsourcing results from variation in asset specificity. Asset specificity refers to transaction costs that occur due to the nature of the products and services being exchanged between buyers and sellers and the potential for these products and services to be redeployed for other purposes.[61] If asset specificity is low, goods and services produced as part of a contractual agreement can be redeployed easily for alternative purposes by different users without significant reduction of value. However, if goods and services arising from a contractual agreement are highly specialized—and have little utility outside an existing contractual arrangement—asset specificity is high and may result in increased levels of dependency by one or both parties due to sunk costs associated with the contract.[62]

Asset specificity can take numerous forms; among those most commonly identified in previous literature are human asset specificity and physical asset specificity.[63] Human asset specificity refers to skills, knowledge, experience, and intellectual property that are unique to a bilateral contractual relationship.[64] In agreements characterized by high human asset specificity, knowledge-related products that emerge from a contract are limited in use outside a unique buyer-supplier relationship. Physical asset specificity refers to products and equipment used to fulfill the terms of a contractual agreement. Physical goods designed for a specific transaction that cannot be redeployed for other economic purposes are characterized by high asset specificity.[65]

To reduce the transaction costs associated with outsourcing, principals often adopt a number of strategies. Chief among these is repeating contractual agreements with the same supplier. In many instances, transaction costs associated with outsourcing can be reduced if screening and oversight regimes between buyers and sellers are standardized over time.[66] Frequent transactions improve monitoring ability and reduce information asymmetries, allowing principals to more accurately assess the performance of agents. However, recurring contracting may also lead to alternate types of inefficiencies. Foremost among these hazards is the possibility that buyers will no longer seek competitive bids for a specific good or service due to the perceived costs of screening alternate suppliers. Therefore, in some cases, failure to engage in competitive bidding in an effort to reduce transaction costs may inadvertently result in adverse selection.

Previous literature examining defense outsourcing through the lens of transaction cost economics has identified several important characteristics of American defense markets that make contracting in the industry unique. First, many markets for defense-related goods and services are monopsonies.[67] That is, the government is the dominant buyer in the field and can use its leverage to influence contracting processes and aspects of corporations' market conduct.[68] Second, adverse selection occurs frequently in defense procurement because government agencies lack sufficient technical knowledge to discern accurately the capabilities of rival firms competing for contract awards.[69] Adverse selection may occur even in mature weapons acquisition and hardware markets due to the rapidly changing nature of some technologies. To reduce information asymmetries, government agencies often seek repeated contracting with the same corporations. This trend toward frequency, however, can lead to bilateral monopolies, which may result in agency dependence on a single contractor.[70] Third, asset specificity presents particular challenges to the defense industry. Many goods and services produced from agreements between government agencies and defense contractors have high asset specificity, meaning they have limited practical value outside their existing contractual arrangements.[71] As previous research has noted, much military training has limited applicability in commercial markets, and certain military hardware such as missiles, tanks, and submarines has almost no use outside national defense settings.[72]

To summarize, contractual agreements between government agencies and companies comprise the primary framework used to manage defense outsourcing. Transaction cost economics and principle-agent theory—two bodies of research previously used to assess the contracting practices of government bureaucracies—provide a useful foundation to explain the behavior of corporations and features of markets within the American defense industry. While previous research has leveraged these theories to examine defense procurement broadly, analysts have not used transaction cost economics to assess the markets for cyber operations, which possess characteristics that make them distinct from other sectors of the defense industry.

Theorizing Contracting Efficiency in United States Cyber Markets

As outlined in the previous section, contracting efficiency varies based on the number of buyers and sellers in a market, a market's maturity, and the types of goods and services being exchanged. Competitive markets in which buyers and sellers have longstanding relationships and where goods exchanged can be easily repurposed are likely to be efficient. By contrast,

nascent markets with few suppliers and high levels of asset specificity are more likely to be characterized by high transaction costs. This section identifies the structural economic features of the cybersecurity, offensive cyber, and data analytics markets and uses this information to develop theory about how these markets function. Table 1 summarizes these arguments.

Table 1. Contracting efficiency in US national security cyber markets

		Adverse Selection	
		Low	High
Asset Specificity	High		Offensive Cyber Operations
	Low	Cybersecurity	Data Analytics/Machine Learning

Because the federal market for cybersecurity has existed for over 20 years—allowing for frequent interactions between corporations and government agencies responsible for American national security—outsourcing in this market is likely to be characterized by low levels of adverse selection.[73] Furthermore, repeated agreements between federal agencies and major defense contractors operating in the cybersecurity market reduce information asymmetries and allow for regularized monitoring and assessment regimes to exist. Additionally, asset specificity in the cybersecurity market is likely to be low because technologies developed for defensive cyber operations can be redeployed for commercial use in the private sector and for use in government agencies outside the national security community. For all these reasons, transaction costs in the cybersecurity market are likely to be low. This does not signify that adverse selection will never occur in the cybersecurity market; however, the structural features of the field indicate that it will operate more efficiently than other national security cyber markets.

In contrast to the cybersecurity market, the offensive cyber market is likely to be characterized by significant transaction costs due to high levels of adverse selection and high asset specificity. Contractors have participated in offensive cyber operations for only a few years. This limits information about companies' comparative capabilities and increases the possibility that information asymmetries exist between government agencies and suppliers. Additionally, asset specificity in the offensive cyber market is likely to be high because offensive missions often involve development of unique code used to enter the cyberspace of disparate adversaries. For this reason, the tools created as part of offensive cyber contracts have limited applicability outside their specific mission environments. Additionally, because the field is highly classified and involves covert operations in which corporations help government employees penetrate the cyberspace

of adversaries—including rival states—many companies will refrain from entering the offensive cyber market. Furthermore, participation in the market is limited by legal barriers such as the Computer Fraud and Abuse Act (CFAA), which restricts offensive cyber operations to United States government entities and their mission partners.[74] Therefore, as the offensive cyber market develops, it will exhibit only moderate levels of competition and is likely to become an oligopoly on the supply side.

Finally, the market for data analytics is likely to be characterized by moderate transaction costs. More so than other federal cyber markets, data analytics has seen the rapid emergence of start-up firms that specialize in niche services. Because the application of machine learning technologies to cyber operations is a new field, adverse selection in the market is likely to be high. Furthermore, because machine learning has a broad range of applications in both cyber and kinetic domains, outsourcing will likely take place with many different companies across numerous national security agencies. In this type of market, agencies are apt to make suboptimal contracting decisions because they lack information about suppliers that comes through years of repeated contracting. However, unlike in the offensive cyber market, asset specificity in the analytics market is low because the tools and technologies developed by companies have broad use in commercial sectors. This market feature means that neither bilateral monopolies nor government dependence on a small number of contractors is likely to develop. Therefore, as contracting in the field becomes more routinized over time, adverse selection in the data analytics market should decrease, and the market will function more efficiently.

Evaluating the Theory by Examining Bid Protests

This inquiry empirically assesses one type of transaction cost present in government cyber markets: adverse selection. Measuring adverse selection can be challenging because the concept possesses an implied counterfactual. That is, an assertion that adverse selection has occurred in a contract award infers that another company could have executed the contract's terms in superior fashion for the same cost.[75] Of course, this type of claim is not verifiable unless an agency hires multiple contractors to perform an identical task for the same fee—an event that rarely occurs outside the early stages of R&D projects or weapons prototyping.[76] In United States defense procurement, however, a formal review process exists whereby companies may protest contracting decisions made by government agencies. If a company believes that an agency has made an error in its award decision, it may file a bid protest with the United States Government

Accountability Office (GAO), which then reviews the contract solicitation process in an "objective, independent, and impartial" manner.[77]

A bid protest automatically halts implementation of a contract until the dispute is reviewed and closed by the GAO.[78] If the GAO finds that a government agency acted improperly or violated federal procurement law as part of the award process, it may sustain a protest and subsequently issue appropriate corrective action, which can include termination of an improperly awarded contract. The GAO's oversight function serves as an internal check on government contracting inefficiencies, especially with respect to adverse selection. Cases in which the GAO sustains protests—such as for lack of fair competition or for incorrect assessment of companies' technical capabilities—strongly indicate that adverse selection has occurred in the procurement process.

If the GAO denies a protest, companies may still seek relief in the courts. The United States Court of Federal Claims (COFC) hears cases in which corporations believe that procurement law or policy has been violated by a government agency. While relatively few companies file complaints with the COFC, it stands as a second level of review and oversight for government contracting award decisions. If the COFC sides with a company opposing a contract awarded by a government agency, then it is likely that adverse selection occurred in that award. Decisions rendered by the COFC are considered final and are almost never appealed to the United States Court of Appeals or United States Supreme Court.[79]

Bid protest decisions are useful in assessing the prevalence of adverse selection in defense outsourcing. By examining decisions in which the GAO or COFC sustain challenges from protesting companies, government agencies can identify weaknesses in their procurement practices. By contrast, denied protests serve as evidence that agencies are carrying out thorough contract award practices. Transaction cost economics suggests that adverse selection is more prevalent in the data analytics and offensive cyber markets and less widespread in the cybersecurity market. The subsequent section evaluates these expectations by reviewing two significant cases of cyber outsourcing that underwent bid protests.

Case Studies in United States Cyber Outsourcing

The GAO and COFC together review thousands of bid protests annually; however, all defense contracts are not equal in terms of their strategic importance. A majority of bid protests are initiated by businesses seeking to reverse decisions on relatively small-dollar awards.[80] While adverse selection may occur across all types and sizes of contracts, suboptimal award

decisions have the greatest potential to influence American national security on large contracts that outsource key defense responsibilities to corporations. For that reason, this inquiry reviews two major cyber contracts tasking companies with core national security duties. Each case serves as a test to determine if adverse selection occurred during the contract bidding phase. The two contracts examined are the Department of Homeland Security's (DHS) $1.15 billion DOMino contract and the Army's $875 million DCGS-A2 contract.

With respect to market type, DOMino is a cybersecurity contract while DCGS-A2 is a data analytics contract. Therefore, the article assesses outsourcing in two distinct cyber markets. While the DHS's original decision was upheld by the GAO in the DOMino award, the COFC agreed with a complaint filed against the Army on the DCGS-A2 contract. Therefore, evidence exists that a suboptimal contracting decision was made on the DCGS-A2 analytics contract, while the GAO's decision in denying a protest on the DOMino award indicates that the correct decision was made on that cybersecurity contract. These findings support arguments previously advanced in the inquiry that predict efficient contracting in the cybersecurity market and less efficient contracting in the field of data analytics.

Ideally, the market for offensive cyber services would also have been examined in this study; however, to date there are no publicly available bid protest decisions for offensive cyber contracts.[81] Activities within the offensive cyber field remain highly classified, and information about the private sector's involvement in offensive cyber operations is therefore limited. Although this inquiry cannot empirically evaluate offensive cyber outsourcing, it is the first study to develop a theoretical framework for assessing economic aspects of the offensive cyber market. In the future, as additional information about offensive cyber outsourcing becomes available, the theory advanced in this article can undergo empirical assessment.

Finally, while the two case studies in this section provide supporting evidence for the inquiry's arguments, they do not serve as a comprehensive test of the article's theoretical claims. Rather, the case studies are exploratory in nature and serve to advance theory development by identifying contracting processes in cyber markets that may lead to inefficient outsourcing.[82] Further investigation of additional cases across the cybersecurity, offensive cyber, and data analytics markets is necessary to evaluate the study's broader assertions. Despite this limitation, the arguments presented in the article serve as an important initial effort to explain features of the markets for defense-related cyber operations performed by corporations.

Development, Operations, and Maintenance Contract

The DOMino contract is a five-year, $1.15 billion cybersecurity award that tasks a corporation with defending over 100 federal computer networks from cyberattacks.[83] The DHS first issued the DOMino request for proposal (RFP) in 2014. The project tasked a contractor to assist the DHS with the design, deployment, operation, and maintenance of the National Cybersecurity Protection System (NCPS), an "integrated system of intrusion detection, analytics, information sharing, intrusion prevention, and core infrastructure capabilities that are used to defend the Federal Executive Branch civilian government's [information technology] infrastructure from cyber threats."[84] The NCPS is essentially an expansive firewall that defends all civilian federal agencies with the .gov domain from malicious cyber activity.[85]

In the DOMino RFP, the DHS highlighted several criteria used to evaluate companies' proposals. Four criteria dealt with technical aspects of DOMino's implementation. These included characteristics of the NCPS system design, ability to integrate the NCPS's capabilities across agencies, operations procedures, and staffing capacity. Additionally, the DHS specified that past contractor performance would be used to assess competing bids. The DHS received proposals from five companies.[86] While the identity of all bidders was not made public because the DOMino review process was managed by the Office of Selective Acquisitions—which supports classified procurements for the DHS—it has been reported that General Dynamics, Leidos, and Lockheed Martin were vying for the award in addition to two publicly confirmed bidders, Raytheon and Northrop Grumman.[87]

In 2015, the DHS awarded the DOMino contract to Raytheon, but Northrop Grumman quickly challenged the award. Northrop's initial challenge resulted in the DHS reevaluating its decision; however, after two reassessments the DHS reaffirmed its award to Raytheon. Northrop subsequently issued another bid protest with the GAO, arguing that awarding DOMino to Raytheon was improper for a number of reasons. Some of Northrop's complaints addressed alleged technicalities and claims of impropriety by Raytheon; however, a significant portion of the protest's content concerned issues related to past performance. Specifically, the DOMino RFP prioritized previous experience in cybersecurity operations "conducting relevant and recent work of the same and or similar nature to the requirements described in the solicitation."[88] Northrop contended that Raytheon had not demonstrated the ability to execute a cyber contract of DOMino's "scope and complexity."[89] Thus, a central component of Northrop's complaint maintained that Raytheon

was a suboptimal prospective supplier because there was insufficient past information establishing that the company could execute a large cyber contract. In effect, Northrop asserted that an information asymmetry existed between the DHS and Raytheon, indicating that it was not possible for the DHS to accurately assess Raytheon's cybersecurity capabilities on a large-scale contract. According to Northrop, Raytheon's lack of previous experience increased the probability that selecting Raytheon to implement DOMino would be an instance of adverse selection.

The GAO's response to Northrop's bid protest evaluated the claim that Raytheon's previous cybersecurity contracting provided insufficient information about the company's ability to execute the DOMino contract. In its evaluation, the GAO noted that Raytheon had relevant experience on three large government cybersecurity projects within the previous five years, collectively totaling $629 million.[90] The GAO also concurred with the DHS's determination that Raytheon's recent cybersecurity work demonstrated "the offeror's ability to successfully perform work under a high dollar value contract."[91] The GAO additionally remarked that Raytheon had performed cybersecurity operations for the FBI and the National Geospatial Intelligence Agency and agreed with the DHS's assessment that this work possessed "the same complexity and scope as the anticipated cybersecurity and operations and management work under the RFP."[92] In brief, in assessing Northrop's claim that Raytheon had insufficient recent experience working on large cybersecurity contracts, the GAO found "no basis to conclude" that the DHS's initial determinations about Raytheon's capabilities were flawed.[93] For this reason, the GAO denied Northrop Grumman's protest, and the DOMino contract was officially awarded to Raytheon.[94]

To summarize, Northrop Grumman challenged the DHS's award of the $1.15 billion DOMino cybersecurity contract to its competitor Raytheon on the grounds that Raytheon had not demonstrated the ability to execute a large cybersecurity project. However, because the federal cybersecurity market has been in existence for decades and numerous companies in the field have worked on prior contracts, government agencies have substantial information about suppliers' capabilities. Therefore, when reviewing proposals, the DHS was able to assess information about contractors' past cybersecurity performance and capabilities. The GAO's review of Northrop's bid protest found that Raytheon had previously executed large cybersecurity contracts of similar scope and scale to DOMino and, based on Raytheon's previous work, agreed with the DHS that the company had the capacity to execute DOMino. While there is no definitive

way to know that Raytheon was a superior supplier to Northrop Grumman, the GAO's review of the DHS's award procedure, coupled with the fact that both the DHS and GAO had substantial information about Raytheon's and Northrop Grumman's cybersecurity capabilities, reduces the likelihood that adverse selection occurred as part of the DOMino contract award process.

Distributed Common Ground System 2 Contract

The Army issued the DCGS-A2 RFP in December 2015. The contract is an extension of the DCGS-A Increment 1 (DCGS-A1) contract, which called for the development of a mobile intelligence, surveillance, and reconnaissance (ISR) analytics platform of software and hardware that would improve Soldiers' "seeing and knowing" on the battlefield—augmenting troops' situational awareness and thus enhancing tactical options and combat capabilities.[95] The DCGS system is intended to combine "all intelligence software/hardware capabilities within the Army into one program."[96] Thus, it is an analytics platform that can both analyze and visualize data, providing troops in the field and Army command personnel with vital ISR information in real time via a shared network. The Army views successful implementation of the DCGS as essential to its missions and deploys the system worldwide in all theaters of operation.[97] The system is therefore a key cyber component of United States national security operations.

DCGS-A1 comprised initial efforts to develop and implement the DCGS system. Principal companies involved in the program included Lockheed Martin and Raytheon, which both worked for over a decade on the project.[98] Although DCGS-A1 resulted in the development and deployment of an operational platform for troops on active duty, its introduction into the battlefield was met with negative assessments. For instance, after the platform was made available to units in Afghanistan, Soldiers from the 130th Engineering Brigade reported that the software was "unstable, slow . . . and a major hindrance to operations."[99] The Army Test and Evaluation Command reviewed initial iterations of the DCGS and found them to have "limitations"; it determined that the system had "poor reliability" and was ultimately "not survivable" due to its excessive complexity and "network vulnerabilities."[100] In 2014, after numerous software updates attempting to fix the DCGS platform, an internal Army review found that the system could not consistently print documents, locate files, maintain a functioning server, or perform search functions.[101] As a result of DCGS-A1's shortcomings, the DCGS-A2 solicitation called for "development of

a new data architecture" that would include cutting-edge "analytical tools, cloud computing, and 'big data' analytic capabilities."[102]

Before the Army could review offerors' proposals for DCGS-A2, Palo Alto–based technology firm Palantir Technologies Inc. submitted a pre-award bid protest to the GAO. Palantir argued that the terms of the DCGS-A2 RFP were illegal because they expressly prohibited use of a commercially available product as part of the DCGS's core system.[103] This provision would prevent Palantir from competing for the DCGS-A2 award.[104] Rather than developing an entirely new data analytics platform, Palantir argued that its existing product—Palantir Gotham—was already in use by several defense and intelligence agencies and could be adjusted to perform the core analytic functions outlined in the DCGS-A2 RFP. From Palantir's perspective, adoption of an existing software platform with a proven record of success represented a superior option for the Army versus creating an entirely new DCGS system.[105]

Palantir made two claims about adverse selection in its protest. First, the company argued that a data analytics system it had already developed was superior to the existing DCGS and would be superior to competitors' efforts to develop a new system. Second, Palantir claimed that selecting a commercially available "off the shelf" system would save the Army both time and money because less labor would be required to modify an existing platform than to develop a new DCGS system from scratch.

Palantir's pre-award bid protest was denied by the GAO; however, the company subsequently sued the Army in the COFC, asking for an injunction halting solicitation on the DCGS-A2 contract.[106] In the suit, Palantir elaborated on arguments it made to the GAO, stressing that its existing software could meet most of the contract's provisions. Specifically, Palantir included testimony from engineers who had reviewed the DCGS-A2 RFP and had knowledge of Palantir Gotham's data analytic capabilities. In assessing Palantir's ability to meet the DCGS-A2 contract's key terms, one expert concluded, "All of these capabilities are available through the commercial marketplace—at a minimum, they are available from Palantir, which is able to provide each of these functions through the Palantir Gotham platform."[107] As it had previously argued to the GAO, Palantir also contended that developing a new data architecture platform from scratch "will result in failure" and will "lock the Army into an irrelevant and unusable 'flagship' intelligence architecture for the next decade."[108]

In November 2016, the COFC ruled in Palantir's favor and issued an injunction ordering the Army to cease procurement efforts for the DCGS-A2 contract until its solicitation terms complied with United States law

and allowed commercially available products to be considered for the award.[109] In its decision, the COFC found that even the Army's own technical experts could not conclusively refute Palantir's ability to perform most duties outlined in the DCGS-A2 RFP.[110] Furthermore, the COFC noted that "it would be wise for the Army to seriously consider reviewing the commercially available products of Palantir, or any other potential offeror, before concluding that no commercially available product can meet the Army's requirements."[111] Therefore, while the COFC did not assert that Palantir Gotham represented a superior product, it ordered the Army to open the DCGS-A2 award to competition so that a more thorough evaluation of all potential offerors' capabilities could take place. The COFC's order thus implied that without increased competition the likelihood of adverse selection was high.

In 2018, after revising the DCGS-A2 RFP to allow companies with commercially available software to compete for the award, the Army chose Palantir and Raytheon—among eight original offerors—to demonstrate their prototypes to Soldiers in a simulated battlefield exercise.[112] After receiving feedback from Soldiers and reviewing proposals from both companies, in 2019 the Army awarded the DCGS-A2 contract to Palantir.[113] In 2020, Palantir was subsequently chosen to continue work on the DCGS system through an $823 million extension known as Capability Drop 2.[114] The company was also recently awarded its first major contract with the Navy, again defeating Raytheon to implement a data analytics project.[115]

In summary, the application of data analytics to military and intelligence operations is an emerging cyber service area. Because it is a relatively new market, government agencies have limited information about corporations' capabilities. Palantir's potential exclusion from consideration for the DCGS-A2 contract meant that the Army would have failed to evaluate a proposal from a qualified supplier that had existing business with the CIA and United States Special Operations Command. This increased the likelihood that adverse selection could occur. If Palantir had not ultimately protested the RFP's terms in court, the DCGS-A2 contract could have been awarded to an inferior supplier, and a clear instance of adverse selection would have taken place. This might have seriously hampered the Army's efforts to develop a state-of-the-art data analytics and visualization platform.

Conclusion

Cyber operations represent the latest strategic domain in which United States military and intelligence agencies have outsourced key national

security responsibilities. This inquiry argues that outsourcing across all cyber markets is not identical. This reality should inform policy makers' management of this growing service area. Cybersecurity is the most developed and competitive cyber market and thus poses the lowest risk for inefficient outsourcing. Owing to decades of repeated contracting, information about the capabilities of corporations active in the cybersecurity market is readily available. Consequently, government agencies outsourcing cybersecurity capabilities are less likely to make suboptimal choices when selecting suppliers and are better able to monitor contractors' performances after agreements are executed. Conversely, the offensive cyber operations market is a new service area with only a small number of companies active in the field. Additionally, the tools that firms develop as part of offensive cyber operations have limited applications outside national security settings. For these reasons, the offensive cyber market risks developing into an oligopoly: a market structure that increases government dependence on a small number of firms. Finally, like the offensive cyber market, the application of data analytics and machine learning to defense and intelligence operations is a new field. For this reason, information about companies' relative capabilities is difficult for government agencies to assess accurately, signifying that rates of adverse selection are likely high. However, there are numerous suppliers in the data analytics market, and services provided by companies in the sector have utility outside national defense settings. Thus, contracting efficiency in the analytics market should improve over time.

Going forward, American leaders must make important policy choices about the trajectory of cyber outsourcing. Two key policy guidelines emerge from this study's arguments. First, outsourcing offensive cyber operations poses both economic and legal risks. The structure of the offensive cyber market and the nature of the tools produced in the field predispose it to inefficiency. Legally, contractors risk taking part in inherently governmental functions if their work on offensive cyber missions directly results in casualties. This means defense agencies should retain—or insource if necessary—the capacity to conduct most aspects of offensive cyber operations. Second, because the data analytics market is made up of many nontraditional defense contractors, it is imperative that the DOD and other agencies look beyond established suppliers to ensure they procure services from the most qualified companies. The DCGS-A2 case demonstrates that agencies may have difficulty evaluating the relative capabilities of companies in the analytics field, while also favoring established defense contractors over new entrants to the marketplace. If the national security

community seeks access to the best analytics and machine learning technologies, it must be more open to working with nontraditional suppliers. The CIA and DOD have recently made efforts to access technologies emerging in start-up businesses through initiatives such as In-Q-Tel and the Defense Innovation Unit (DIU); however, major obstacles still exist for commercial firms seeking to work in the defense industry.[116]

In conclusion, as technology becomes increasingly central to national security, corporations are likely to assume a more central role in military and intelligence operations. While cooperation with the private sector contributes to American defense capabilities, the DOD and the intelligence community must continue to implement rigorous procurement practices to ensure they hire the most capable service providers and monitor contractors' performances meticulously. This will prove challenging as new suppliers of cybersecurity and other technology services seek to enter the rapidly growing United States defense market.[117] To successfully navigate future outsourcing challenges, the national security community will need to balance the entrance of major commercial technology firms like Amazon and Microsoft with agencies' existing relationships with traditional defense contractors such as Raytheon and Northrop Grumman. Additionally, the DOD should make further efforts to access cutting-edge innovations emerging from smaller technology firms while overcoming any lingering anti-defense bias that exists in some commercial circles. Historically, the partnership between the United States' dynamic businesses and the national security community has been a strategic asset. To make sure this pattern carries on in cyberspace and beyond, the DOD and the intelligence community should continue to innovate their outsourcing practices while carefully monitoring and evaluating the work defense contractors perform. SSQ

Charles W. Mahoney

Dr. Mahoney is an associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals.

Notes

1. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, 2018), https://dod.defense.gov/.

2. Kristen E. Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* 95, no. 3 (2017): 467–538, http://texaslawreview.org/. Cybersecurity partnerships between governments and the private sector also may occur on an ad hoc basis.

3. Exceptions include Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2018), 71–80; Martin Libicki, David Senty, and Julia Pollack, *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND, 2014), https://www.rand.org/; and Irving Lachow and Taylor Grossman, "Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, eds. Herbert Lin and Amy Zegart (Washington D.C.: Brookings Institution Press, 2018), 379–401.

4. Eugene Gholz and Harvey Sapolsky, "Restructuring the U.S. Defense Industry," *International Security* 24, no. 3 (1999): 5–51, https://www.belfercenter.org/; P. W. Singer, *Corporate Warriors*: *The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2003); Deborah Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge, MA: Cambridge University Press, 2005); and Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (New York: Oxford University Press, 2014).

5. Eugene Gholz and Harvey M. Sapolsky, "The Very Healthy US Defense Innovation System," UC San Diego Study of Information and Technology in China (SITC) Research Briefs, Series 10: Defense Innovation, 2018-5, https://escholarship.org/.

6. Rhys McCormick, *Defense Acquisition Trends 2019: Topline DoD Trends* (Washington, D.C.: Center for Strategic & International Studies, 2019), https://www.csis.org/; Moshe Schwartz, John F. Sargent Jr., and Christopher T. Mann, *Defense Acquisitions: How and Where DoD Spends Its Contracting Dollars* (Washington, DC: Congressional Research Service, 2018), https://fas.org/; Allison Stanger, *One Nation Under Contract: The Outsourcing of American Power and the Future of American Foreign Policy* (New Haven, CT: Yale University Press, 2009); and Laura A. Dickinson, *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven, CT: Yale University Press, 2011).

7. Schwartz, Sargent, and Mann, *Defense Acquisitions*, 1.

8. Govini, *Federal Cybersecurity: FY18 Standard Market Taxonomy of Unclassified Spending* (Alexandria, VA: Govini, 2017), 1. Govini is a data analysis company that performs work for various United States defense agencies. The data the firm receives and analyzes comes directly from government departments and agencies.

9. The DOD makes a distinction between defensive cyber operations and securing the Department of Defense Information Network (DODIN). For the purposes of conceptual parsimony, this inquiry merges these two activities.

10. It can be difficult to distinguish offensive and defensive operations in cyberspace. For more on this topic, see Eric Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyber Space," *Security Studies* 24, no. 2 (2015): 316–48.

11. Joint Publication (JP) 3-12, *Cyberspace Operations*, 8 June 2018, II-5, https://www.jcs.mil/.

12. JP 3-12, II-5.

13. Govini, *Federal Cybersecurity*, 2.

14. Govini, 2.

15. Booz Allen Hamilton, "Cyber Fusion Center: Next Gen Security Operations," accessed January 2021, https://www.boozallen.com/.

16. General Dynamics, corporate website, accessed January 2021, https://www.gdit.com/.

17. Software engineers often prefer working in the private sector due to more lucrative salaries and greater work flexibility. This has resulted in staffing difficulty at CYBERCOM. See Mark Pomerleau, "The Army's New Multi-Domain Units Are Understaffed," *Fifth Domain*, 15 August 2019, https://www.fifthdomain.com/.

18. Patrick Howell O'Neill, "After a Long Fight, Raytheon Wins $1 Billion Cybersecurity Contract with Homeland Security," *Cyberscoop*, 19 June 2017, https://www.cyberscoop.com/.

19. Mark Pomerleau, "Cyber Command Awards $54M Contract for Cyber Carrier," *Fifth Domain*, 29 October 2018, https://www.fifthdomain.com/.

20. For more on the difficulty the national security community has experienced working with technology firms, see Amy Zegart and Michael Morrell, "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail," *Foreign Affairs* 98, no. 3 (May/June 2019): 85–96, https://www.foreignaffairs.com/.

21. Sharon Weinberger, "The Everything War," *MIT Technology Review* 122, no. 6 (2019): 28, https://wp.technologyreview.com/.

22. Weinberger, 28.

23. Kate Conger, "Judge Halts Work on Microsoft's JEDI Contract, A Victory for Amazon," *The New York Times*, 13 February 2020, https://www.nytimes.com/. In October 2019, the DOD awarded the JEDI contract to Microsoft; however, Amazon challenged the award, and in February 2020, a federal judge halted all work on JEDI pending legal resolution of Amazon's protest.

24. Conger, "Judge Halts Work."

25. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 90–113, https://www.airuniversity.af.edu/.

26. JP 3-12, *Cyberspace Operations*, II-5. The Joint Chiefs of Staff distinguish between blue cyberspace controlled by the DOD and its partners and red cyberspace—which is cyberspace owned or controlled by an adversary. Gray cyberspace refers to all cyberspace that does not meet the description of blue or red cyberspace.

27. Govini, *Federal Cybersecurity*, 1.

28. Lachow and Grossman, "Cyberwar."

29. Justin Lynch, "Security Companies See Opportunity in Trump's New Cyber Plan," *Fifth Domain*, 26 September 2018, https://www.fifthdomain.com/.

30. James Bach, "SAIC Sees Opportunity in Feds 'Offensive Cyber' Efforts," *Washington Business Journal*, 25 May 2016, https://www.bizjournals.com/.

31. James Bach, "Leidos CEO Roger Krone Confirms That Company Does 'Offensive Cyber' for Feds," *Washington Business Journal*, 5 May 2016, https://www.bizjournals.com/.

32. ManTech, corporate website, accessed December 2020, https://www.mantech.com/.

33. CACI, corporate website, accessed December 2020, http://investor.caci.com/.

34. Bach, "SAIC Sees Opportunity"; and SAIC, corporate website, accessed December 2020, https://jobs.saic.com/jobs/.

35. Kate M. Manuel, *Definitions of "Inherently Governmental Function" in Federal Procurement Law and Guidance* (Washington, D.C.: Congressional Research Service, 2014), https://digital.library.unt.edu/.

36. For more on the legal definition of inherently governmental functions, see John R. Luckey, Valerie Baily Grasso, and Kate M. Manuel, *Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress* (Washington, D.C.: Congressional Research Service, 2009), https://fas.org/.

37. Renée De Nevers, "Private Security Companies and the Laws of War," *Security Dialogue* 40, no. 2 (April 2009): 169–90, https://doi.org/10.1177/0967010609103076.

38. Manuel, *Definitions of "Inherently Governmental Function,"* 3.

39. John S. Hurley, "Enabling Successful Artificial Intelligence Implementation in the Department of Defense," *Journal of Information Warfare* 17, no. 2 (2018): 65–82, https://www.jstor.org/stable/26633155?seq=1.

40. Zak Doffman, "Russia Unleashes New Weapons in Its Cyberattack Testing Ground," *Forbes*, 5 February 2020, https://www.forbes.com/.

41. Office of the Director of National Intelligence, *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, D.C.: Office of the Director of National Intelligence, 2019), https://www.dni.gov/.

42. Govini, *Federal Cybersecurity*, 16. Govini's data on analytics tracks spending on cyber related analytics contracts and not on all federal spending on AI and machine learning technologies, which is likely much higher.

43. Govini, 16.

44. Govini, 16.

45. Charles W. Mahoney, "Acquire or Expire: Publicly Traded Defense Contractors, Financial Markets, and Consolidation in the U.S. Defense Industry," *Defence and Peace Economics*, 2019, https://doi.org/10.1080/10242694.2019.1667216.

46. For more on the relationship between Palantir and In-Q-Tel, see Peter Waldman, Lizette Chapman, and Jordan Robertson, "Palantir Knows Everything About You," *Bloomberg Businessweek*, 19 April 2018, https://www.bloomberg.com/; and Murad Ahmed, "Palantir Goes from CIA Funded Start-Up to Big Business," *Financial Times*, 24 June 2015.

47. Ken Dilanian, "US Special Operations Forces are Clamoring to Use Software from Silicon Valley Company Palantir," *Business Insider*, 26 March 2015, https://www.businessinsider.com/; and Palantir, "Fielding an Advanced Analytic Capability in a Warzone," accessed December 2020, https://www.palantir.com/.

48. Kate Fazzini and Amanda Macias, "Peter Thiel's Company Palantir Just Won a Major Pentagon Contract, Beating Out Traditional Military Vendors," *CNBC*, 27 March 2019, https://www.cnbc.com/.

49. Palantir, corporate website, accessed January 2021, https://www.palantir.com/.

50. Palantir, corporate website.

51. Aaron Gregg and Douglas MacMillan, "Palantir Goes Public at $10 Dollars per Share," *The Washington Post*, 1 October 2020, https://www.washingtonpost.com/.

52. Lindsey R. Sheppard, *Artificial Intelligence and National Security: The Importance of the AI Ecosystem* (Washington, DC: Center for Strategic and International Studies, 2018), https://www.csis.org/.

53. Graham Allison, "Is China Beating America to AI Supremacy?," *The National Interest*, 22 December 2019, https://nationalinterest.org/.

54. James Vincent, "Putin Says the Nation That Leads in AI 'Will be the Ruler of the World,'" *The Verge*, 4 September 2017, https://www.theverge.com/.

55. All organizations—within and outside government—must choose what goods and services they will produce internally and what inputs and operations they will outsource. Even organizations with high levels of vertical integration typically outsource important aspects of their operations. This "make or buy" decision is foundational to the field of transaction cost economics. For more on this body of work, see Ronald Coase, "The Nature of

the Firm," *Economica* 4, no. 16 (1937): 386–405, https://doi.org/10.1111/j.1468-0335.1937.tb00002.x; Ronald Coase, "The Problem of Social Cost." *Journal of Law and Economics* 3 (1960): 1–44, https://www.law.uchicago.edu/; and Oliver Williamson, "The Economics of Organization: The Transaction Cost Approach," *The American Journal of Sociology* 87, no. 3 (November 1981): 548–77, https://doi.org/10.1086/227496.

56. Robert J. David, "A Systematic Assessment of the Empirical Support for Transaction Cost Economics," *Strategic Management Journal* 25, no. 1 (2004): 39–58, https://doi.org/10.1002/smj.359.

57. For a discussion of transaction cost economics and its application to public bureaucracies, see Oliver E. Williamson, "Public Bureaucracies: A Transaction Cost Economics Approach," *The Journal of Law, Economics, & Organization* 15, no. 1 (April 1999): 306–42, https://www.jstor.org/stable/3554953?seq=1.

58. Oliver E. Williamson, "Transaction Cost Economics: How It Works, Where It Is Headed," *De Economist* 146, no. 1 (1998): 23–58, https://doi.org/10.1023/A:1003263908567.

59. Peter Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, MA: Harvard University Press, 2003), 74.

60. James Cockayne, "Make or Buy? Principal-Agent Theory and the Regulation of Private Military Companies," in *From Mercenaries to Markets: The Rise and Regulation of Private Military Companies*, eds. Simon Chesterman and Chia Lehnardt (Oxford: Oxford University Press, 2007), 197.

61. The term "asset specificity" was coined by Oliver E. Williamson. For more on the topic see Oliver E. Williamson, *The Economic Institutions of Capitalism* (New York: Free Press, 1985).

62. Chris Lonsdale, "Locked-In to Supplier Dominance: On the Dangers of Asset Specificity for the Outsourcing Decision," *Journal of Supply Chain Management* 37, no. 2 (Spring 2001): 22–27, *Gale Academic OneFile*, accessed 22 January 2021, https://go.gale.com/.

63. Other types of asset specificity include site asset specificity, temporal asset specificity, and brand asset specificity. For more on conceptualization of asset specificity, see Glauco De Vita, Arafet Tekaya, and Catherine L. Wang, "The Many Faces of Asset Specificity: A Critical Review of Key Theoretical Perspectives," *International Journal of Management Reviews* 13, no. 4 (2011): 329–48, https://doi.org/10.1111/j.1468-2370.2010.00294.x.

64. Gordon Walker and David Webber, "A Transaction Cost Approach to Make-or-Buy Decisions," *Administrative Science Quarterly* 29, no. 3 (1984): 373–91, https://doi.org/10.2307/2393030.

65. Paul L. Joskow, "Asset Specificity and the Structure of Vertical Relationships: Empirical Evidence," *Journal of Law, Economics, and Organization* 4, no. 1 (1988): 95–177, http://www.jstor.org/stable/765016.

66. De Vita, Tekaya, and Wang, "The Many Faces of Asset Specificity," 329–48.

67. Charles W. Mahoney, "Buyer Beware: How Market Structure Affects Contracting and Company Performance in the Private Military Industry," *Security Studies* 26, no. 1 (2017): 30–59, https://doi.org/10.1080/09636412.2017.1243912.

68. Keith Hartley, "The Arms Industry, Procurement and Industrial Policies," in *Handbook of Defense Economics: Defense in a Globalized World*, eds. Todd Sandler and Keith Hartley (New York: North Holland, 2007), 1161.

69. Todd Sandler and Keith Hartley, *The Economics of Defense* (New York: Cambridge University Press, 1995), 127–28.

70. Sandler and Hartley, 127–28.

71. Raymond Franck and Francois Melese, "Defense Acquisition: New Insights from Transaction Cost Economics," *Defense & Security Analysis* 24, no. 2 (2008): 107–28, https://doi.org/10.1080/14751790802124931.

72. J. Eric Fredland, "Outsourcing Military Force: A Transactions Cost Perspective on the Role of Military Companies," *Defence & Peace Economics* 15, no. 3 (2004): 205–19.

73. Maurer, *Cyber Mercenaries*, 71.

74. The CFAA was first enacted in 1986 and last amended in 2008. See Cornell Law School, Legal Information Institute, 18 U.S. Code § 1030 – Fraud and related activity in connection with computers, https://www.law.cornell.edu/.

75. This type of implied counterfactual claim is common in social science research and relates to the "fundamental problem of causal inference," which argues that there will always be uncertainty underlying causal claims in the social sciences because history cannot be rerun in order to assess the precise effect the presence or absence of a specific independent variable has on an observed outcome. For more on this topic, see Paul W. Holland, "Statistics and Causal Inference," *Journal of the American Statistical Association* 81, no. 396 (1986): 945–60, https://doi.org/10.1080/01621459.1986.10478354; Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry: Scientific Inquiry in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994), 76–82; and James D. Fearon, "Counterfactuals and Hypotheses Testing in Political Science," *World Politics* 43, no. 2 (1991): 169–95, https://doi.org/10.2307/2010470.

76. While the DOD and other government departments can try and avoid adverse selection through R&D projects and competitive prototyping, it is not possible to carry out controlled comparisons for all the major procurement RFPs government agencies issue on an annual basis.

77. The GAO has formally handled the federal bid protest process since 1984 when Congress passed the Competition in Contracting Act with the goal of increasing transparency in the government's contracting process. For more on the bid protest process, see GAO's website, https://www.gao.gov/legal/bid-protests.

78. Mark V. Arena et al., *Assessing Bid Protests of U.S. Department of Defense Procurements: Identifying Issues, Trends, and Drivers* (Santa Monica, CA: RAND, 2018), 9, https://www.rand.org/.

79. Arena et al., 9.

80. Arena et al., xiii–xv. A recent RAND study hypothesized that small companies are more likely to file bid protests because the revenue they stand to lose by not winning an award can pose a serious threat to their continued business operations.

81. Many defense contractors advertise for job openings in the field of offensive cyber operations; however, to date the only publicly awarded contract generally believed to include offensive cyber operations is USCYBERCOM's $460 million 2016 operations support contract, which was awarded to six different corporations. See Aaron Boyd, "CYBERCOM Awards Spots on New $460 Million Cyber Operations Contract," *Federal Times*, 23 May 2016, https://www.federaltimes.com/.

82. For more on exploratory case studies, see John Gerring, *Case Study Research: Principles and Practices* (New York: Cambridge University Press, 2017), 65–83.

83. United States Government Accountability Office (US GAO), *Northrop Grumman Systems Corporation; B-412278.7, B-412278.8* (Washington, D.C.: Comptroller General of the United States, 4 October 2017), https://www.gao.gov/.

84. US GAO, *Northrop Grumman Systems Corporation*.

85. The NCPS is operationally known as the "EINSTEIN set of capabilities" and is often simply referred to as EINSTEIN in government and press publications referencing NCPS.

86. US GAO, *Northrop Grumman Systems Corporation*, 3.

87. Jason Miller, "DHS Awards $1 Billion Cyber Contract to Protect Agency Networks," *Federal News Network*, 23 September 2015, https://federalnewsnetwork.com/.

88. US GAO, *Northrop Grumman Systems Corporation*, 17.

89. US GAO, 17.

90. US GAO, 17.

91. US GAO, 18.

92. US GAO, 18.

93. US GAO, 18.

94. US GAO, 21.

95. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, No. 16-784C, 3 November 2016, 3, https://ecf.cofc.uscourts.gov/.

96. United States Government Accountability Office, *Palantir USG, Inc.; B-412746* (Washington, D.C.: Comptroller General of the United States, 2016), https://www.gao.gov/.

97. US GAO, *Palantir USG*.

98. Raytheon, "United States Army Analysis and Control Element (ACE) Block II, Distributed Common Ground System—Army (DCGS-A)," case study, 2014, https://www.raytheon.com/; and Lockheed Martin, "U.S. Army Testing Lockheed Martin's Upgrades to Battlefield Intelligence Enterprise," 14 October 2014, https://news.lockheedmartin.com/.

99. Jen Judson, " 'Powerful Tool' but 'Requires Extensive Training': Soldiers Find DCGS-A Hard to Use as Difficulties Hinder Operations," *Inside the Army* 26, no. 6 (2014): 8–9, http://www.jstor.org/stable/24836007.

100. Greg Slabodkin, "Distributed Common Ground System Comes under Fire," *Defense Systems*, 1 October 2012, https://defensesystems.com/.

101. Rowan Scarborough, "Problems with Army's Battlefield Intel System Unresolved after Two Years," *The Washington Times*, 1 May 2014, https://www.washingtontimes.com/.

102. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, 4.

103. Before the Army issued the DCGS-A2 RFP, it conducted a market research review and determined that no commercially available products were suitable for the DCGS platform.

104. US GAO, *Palantir USG, Inc.; B-412746*.

105. US GAO, *Palantir USG, Inc.; B-412746*.

106. Sean Lyngaas, "Palantir to Sue Army over DCGS," *Federal Computer Week*, 20 June 2016, https://fcw.com/articles/.

107. The United States Court of Federal Claims, *Palantir USG Inc. v. United States*, 93.

108. The United States Court of Federal Claims, 16.

109. The United States Court of Federal Claims, 104.

110. The United States Court of Federal Claims, 94.

111. The United States Court of Federal Claims, 96.

112. Nick Wakeman, "Palantir, Raytheon to Battle Under $876m Army DCGS-A Contract," *Washington Technology*, *WT Business Beat* (blog), 12 March 2018, https://washingtontechnology.com/.

113. Shane Harris, "Palantir Wins Competition to Build Army Intelligence System," *Washington Post*, 26 March 2019, https://www.washingtonpost.com/.

114. Jackson Barnett, "Palantir, BAE Score $823 Million Contract to Modernize Army's Distributed Common Ground System," *Fedscoop,* 26 February 2020, https://www.fedscoop.com/.

115. Aaron Gregg, "Palantir Seals Its First Major U.S. Navy Deal as Raytheon Is Passed Over," *The Washington Post*, 5 March 2020, https://www.washingtonpost.com/.

116. In 2016, the Pentagon announced the formation of the Defense Innovation Unit (DIU), a DOD organization tasked with helping the military gain access to cutting-edge technological innovation in the private sector. For more on the DIU see Aaron Metha, "Former Symantec Boss Takes Over at Defense Innovation Unit," *Defense News*, 24 September 2018, https://www.defensenews.com/.

117. DOD outlays on defense contractors totaled $402 billion in 2019. See Daniel Snyder, "Federal Contract Spending: Five Trends in Five Charts," *Bloomberg Government*, 6 January 2020, https://about.bgov.com/.

Europe as a Secondary Theater? Competition with China and the Future of America's European Strategy

Luis Simón
Linde Desmaele
LTC Jordan Becker, USA

Abstract

Competition with China has become the main lens through which the United States looks at the world. How will this affect US strategy in Europe? First, Washington's increased focus on China leaves fewer US resources available to influence security developments in and around Europe. This compels US policy makers to seek ways to preserve a favorable regional balance in Europe that require less of the United States. Second, Sino-American competition is leading Washington to view its transatlantic relationships in terms of how they affect its position relative to China. As the Euro-Atlantic area becomes less central to US grand strategy, global—and particularly China-focused—considerations will play an increasingly important role in the context of the transatlantic relationship.

*****

The United States has steadily shifted strategic attention toward China and Asia since the end of the Cold War.[1] However, US strategists long argued that the US and China shared an interest in "sustain[ing] . . . the international . . . system that has enabled [China's] success."[2] The Trump administration, in contrast, was the first to define America's relationship with China in unambiguously competitive terms, referring to China as a "long-term strategic" competitor seeking to "substantially revise the post–Cold War international order and norms of behavior."[3] Bipartisan support for this approach means that the decision to put global competition with China at the center of US grand strategy may turn out to be President Trump's main foreign policy legacy.[4] Critically, the notion that the United States finds itself in strategic competition with China appears to have won strong support among Democrats,[5] with

the Obama administration's senior China advisor describing competition with China as "more of a condition than a strategy"[6] and the party's 2020 platform urging that the United States must "stand up to China" to "shape the unfolding Pacific century."[7]

As competition with China becomes increasingly central to US grand strategy, the United States is likely to look at different regions and relationships across the world through the lens of that competition.[8] How is competition with China likely to affect US strategy in Europe? We argue that a stable Europe is a precondition for the US to marshal diplomatic, economic, and military resources to compete with China. This means that the US both seeks to ensure a favorable balance of power in Europe and to enlist European support in its rivalry with China. Thus, two sets of challenges exist for the United States going forward.

First, to influence and maintain a favorable balance of power in Europe, Washington has traditionally relied on a strategy of forward military presence coupled with economic and diplomatic engagement. But US resources are limited, and increasing demand for them in Asia raises new questions about whether Washington can preserve a favorable European regional balance at a lower cost than in the past. In this context, Washington must consider how much influence it is willing to cede to European actors, including Germany, Russia, Britain, France and the European Union (EU).

Second, as Europe becomes a secondary theater in US grand strategy, Washington is compelled to ensure that Europe's key powers and institutions support US interests when it comes to competition with Beijing, or at least that they do not undermine US efforts in this regard. In reframing its relationship with Europe, the US is paying increasing attention to Europe's positions toward China and Asia. Washington recently warned Europeans, for example, about China's efforts to leverage investments and trade to gain technological and related strategic advantages relative to the United States.[9] China-related considerations are also likely to gain relevance in the context of America's calculations vis-à-vis Russia, a country that can play a direct—if limited—strategic role in China's immediate periphery: Central Asia, Northeast Asia, and the Western Pacific. For now, the US continues to look at Russia (primarily) through a European lens and worries about Moscow's potential to threaten US regional interests and upset the European balance. However, as competition with China becomes the focus of US grand strategy, Washington may increasingly consider how Russia can affect that competition—whether through its relationship with China, its ability to strain the European balance of power, or its propensity to create challenges elsewhere in the world.

While it is certainly conceivable that the United States could retain such overwhelming advantages vis-à-vis all its peer competitors, or that China's rise could organically slow or reverse, the US does not seem to be betting on either scenario.[10] The centrality of China in US grand strategy appears to be structural, driven by the broader eastward shift in the distribution of global economic power. It is therefore unsurprising that as the United States becomes increasingly preoccupied with China's rise, it adjusts strategy in other regions accordingly. The fact that Washington has labelled China as a "global" competitor makes it difficult to isolate Sino-American competition in Asia and the broader Indo-Pacific area from what happens in other theaters, particularly Europe.

This article first introduces the notion of Sino-American competition as it relates to Washington's European strategy. Second, we focus on US efforts to maintain a favorable balance of power in Europe and delineate a set of challenges that arise as Washington has fewer resources at its disposal for a proactive role in this regard. Third, we look at Washington's efforts to coordinate with Europeans—allies and adversaries alike—in its rivalry with China. Drawing on an examination of elite discourse, interviews, and existing literature, we demonstrate that Washington's European strategy is today informed by both European and non-European developments. In the conclusion, we briefly summarize our main findings and provide avenues for future research.

Sino-American Competition and US Grand Strategy

The US's post–Cold War strategic reorientation toward Asia has developed over successive administrations of both parties, benefiting from broad elite support.[11] The rise of Asia was a prominent foreign policy theme during the Bush and (especially) Obama administrations, both of which looked at Asia primarily through the lens of economic opportunity. While the Obama administration noted the risks China's rise and military modernization posed to the region's existing security order, it also clung to the notion that economic liberalization would bring about political liberalization and avoided casting its relationship with Beijing in unambiguously competitive terms.[12]

The Trump administration has, though, particularly emphasized the competitive character of the Sino-American relationship and elevated that competition to the center of US grand strategy.[13] The 2017 *National Security Strategy* (NSS) describes China as challenging "American power, influence, and interests . . . across political, economic, and military arenas," aiming "to change the international order in [its] favor."[14] In addition, the

unclassified synopsis of the 2018 National Defense Strategy (NDS) notes that the US seeks to "expand the competitive space" in its relationship with Beijing to "compete, deter, and win."[15] The NSS highlights China's attempts to "displace the United States in the Indo-Pacific region" and "reorder the region in its favor."[16] Against that backdrop, the NDS underscores the importance of "maintaining a favorable balance of power in the Indo-Pacific" and reassuring US allies and partners therein.[17]

The Trump administration did not view competition with China as limited to Asia or even the broader Indo-Pacific, nor as solely military.[18] In fact, it prioritized technological competition. US vice president Mike Pence, for example, strongly denounced ongoing efforts by Chinese state-led companies to access—and eventually dominate—global markets in technologies such as fifth generation (5G) cellular network technology and artificial intelligence (AI).[19] The developed economies and lucrative markets of Europe and East Asia are particularly important in this context.[20]

At the same time, the 2017 NSS and 2018 NDS identify Russia as a strategic competitor and often lump Russia and China together, thus seeming to confound prioritization.[21] US officials want to reassure allies and avoid the appearance of neglecting other regions (including Europe) for the sake of Asia.[22] Yet in their public statements, both President Trump and his senior advisors periodically identify China as the greatest challenge for the United States and the rules-based international order.[23] Secretary of State Mike Pompeo argued that China, not Russia or Iran, constitutes the greatest threat to the West.[24] Similarly, in his remarks to the Senate Armed Services Committee in March 2019, former secretary of defense Patrick Shanahan argued that his main priority is to ensure military overmatch worldwide, but particularly with China, which he described as a "whole-of-government threat to the US."[25] US defense officials have argued that in practice, China is a clear priority.[26] Within the DOD, "Russia is seen as a pretty significant but diminishing threat, whereas China is seen as a growing and long-term threat."[27]

Although critics often point to alleged inconsistencies in the US's China strategy, some of its broad contours have remained rather stable. For one thing, the US appears to have abandoned the prospect of China becoming a "responsible stakeholder" in the (US-led) international order.[28] The US has also emphasized its willingness to counter China's military actions in Asia and across the broader Indo-Pacific region.[29] Such an approach toward Beijing enjoys bipartisan support in Washington, meaning it will likely persist into future administrations—with variations in style but consistency in viewing China as a global competitor.[30]

Because outcompeting China has become its most pressing strategic challenge, Washington is adjusting its policies and relationships elsewhere in the world to ensure that they support competition with Beijing. While the shift has been gradual, it is now apparent; it represents a significant change from the twentieth century when the US went to war twice in Europe and conflicts elsewhere were often driven by the logic of European security. Whereas during the Cold War the US enlisted European allies in a global struggle against a European power, today the US seeks to enlist European allies in a global competition with a non-European power.

To be sure, neither competition with China nor the preservation of a favorable regional balance in the Indo-Pacific fully monopolizes US global strategy. Both the 2017 NSS and the declassified synopsis of the 2018 NDS emphasize America's ongoing commitment to the preservation of "favorable balances of power in Europe and the Middle East."[31] The NSS even refers to Europe as the United States' most "significant trading partner" and notes that America is "safer when Europe is prosperous and stable."[32] Yet there is growing concern in Washington about how China's rise might affect European security. In this regard, the NSS warns about Beijing's supposed efforts to "gain a strategic foothold in Europe by expanding its unfair trade practices and investing in key industries, sensitive technologies and infrastructure."[33] A 2019 task force report published by the bipartisan Asia Society similarly identifies "China's pursuit of a mercantilist high-tech import-substitution industrial policy" and its "economic and diplomatic statecraft to gain a military foothold beyond Asia," including in Europe, as key grand strategic challenges.[34] In other words, because US strategic objectives in Asia and Europe are increasingly interdependent, China and Asia are also becoming increasingly relevant in Washington's dealings with and in Europe. This interdependence complicates America's European strategy in two ways: by underscoring the problem resource trade-offs and by pushing the US to reconcile competing interests across the two regions.

Preserving the European Balance of Power

Ensuring that no single state or coalition of states would dominate either Europe or East Asia has been a top geostrategic priority for the United States since at least the First World War.[35] Europe and East Asia represent the world's greatest concentration of latent power in terms of wealth, demographics, and military-industrial potential.[36] They are also the two parts of the Eurasian "rimland" that have the easiest and most direct access to the continental United States via the Atlantic and Pacific

Oceans.[37] If a single power managed to dominate the resources of either region, it would be in a strong position to challenge the US's global economic and strategic influence and freedom of action. While there has been an isolationist strand in foreign policy thinking since the birth of the United States, successive postwar administrations have embraced the view that maintaining a network of forward bases and alliances in Europe and East Asia is the most efficient way to preserve a favorable balance of power in those regions and mitigate the risk of such a challenge. The primary alternative of "offshore balancing"—basing forces in the US and responding to emergencies as they arise—has not gained much adherence in the US government or with either political party, as it is seen as riskier and more expensive.[38] Scholars who advocate for offshore balancing also recognize this fact, even as they often portray events like the end of the Cold War or the 2008 financial crisis as a window of opportunity for the US to adopt a strategy in line with their prescriptions.

For most of the twentieth century, the US clearly elected not to pursue an offshore balancing strategy in Europe. Since the end of the Second World War, in particular, the United States adopted a proactive, forward-leaning grand strategy in Europe as it sought to manage the only two powers deemed to have the potential to dominate the system: Russia and Germany. After defeating Germany militarily in the Second World War, Washington's immediate priority was to ensure that it would not be in a position to threaten the continental balance again. Yet with Germany militarily and industrially devastated, divided between East and West, and East Germany and most of Eastern and Central Europe under Soviet influence, attention turned toward Moscow—now the greatest threat to the European balance. The United States soon concluded that a friendly and submissive (yet adequately armed) West Germany was the most cost-effective way of balancing the power of Soviet Russia in Central Europe and thus promoted West Germany's reindustrialization and remilitarization.[39] But this strategy required significant US investment and presence in Europe to reassure the rest of the Continent's states: Secretary of State Dean Acheson was concerned about Germany acting as "the balance of power in Europe," and many European allies preferred Germany never to rearm.[40]

Critically, by advancing NATO and the European Community (EC) as mechanisms to oversee the process of West German rearmament and reindustrialization, the United States (and its British and French allies) would ensure that Bonn's potential would work for and not against its interests. America's Cold War European strategy thus followed a logic of

dual containment: the Soviet Union through alliances and deterrence and West Germany by socializing it into the nascent transatlantic community.[41] As the Soviet Union grew more threatening and West Germany socialized into the West, the United States focused increasingly on the need to keep the Soviets out rather than keeping the Germans down. In any event, the preservation of a balance of power in Europe was America's chief global concern throughout the Cold War. This is not to say that Washington did not pay attention to other regions, especially East Asia. But because the strategic competition with Moscow was identified as the top priority of US grand strategy, because Moscow's power base was firmly anchored in Europe, and because Europe was the world's most economically dynamic region outside North America, few US resources were spared when it came to the primary objective of preserving the European balance.[42]

With the implosion of the Soviet Union in the early 1990s, Europe began to progressively lose the centrality it had enjoyed in US grand strategy during the Cold War. But even absent an immediate threat to the balance of power in Europe, policy makers did not seek to shift to a strategy of offshore balancing. After all, Washington's forward presence in Europe continued to provide it with positive leverage over its allies' strategic direction. It also served as a launching pad for US activities elsewhere, especially in the Middle East.[43] In any case, throughout the 1990s and 2000s, the United States seemed to enjoy such overwhelming advantages vis-à-vis all its potential competitors that discussions on resource trade-offs between regions appeared unnecessary. There was a widespread sense that Washington could do anything, everywhere, any time.[44] This unipolar era appears to be waning. The 2017 NSS and 2018 NDS herald the return of great power competition, identifying China and Russia as long-term strategic competitors that are challenging US interests and the balance of power in Europe and the Indo-Pacific simultaneously.[45] More broadly, the United States faces a much less permissive international environment than was the case during the immediate post–Cold War period.[46] Against this backdrop, resource prioritization is an increasingly salient issue.

Additionally, most scholars and experts agree that China poses a more comprehensive long-term challenge for American power than Russia does. Already in 2014, John Ikenberry wrote that it was China's rise that would inevitably bring the United States' unipolar moment to an end.[47] For his part, John Mearsheimer refers to Russia as "by far the weakest of the three great powers for the foreseeable future, unless either the US or Chinese economy encounters major long-term problems." The key question, according to him, is "to determine which side, if any, Russia will take

in the US-China rivalry."[48] But as the United States continues to shift its gaze further eastward, can the stability and presence of friendly powers in Europe be guaranteed without a strong US engagement?

The United States currently faces a strategic dilemma in Europe. On the one hand, the prioritization of China and Asia constrains Washington's ability to engage in Europe, incentivizing it to adopt a more indirect and flexible approach.[49] On the other hand, a significant retrenchment of US power in Europe could leave "too much" space for other players, spurring a process of geopolitical competition that could be damaging to US economic and political interests or, worse still, result in the rise of a dominant power in the Continent. While such risks appear manageable at low cost to offshore balancers, US policy makers disagree. Three powers are particularly relevant in this regard: Russia, Germany, and the prospect of a politically united and strategically autonomous EU.[50]

Europe experts in the United States call attention to the continued importance of Europe-related challenges for US security and prosperity.[51] However, such challenges are no longer at the top of America's grand strategic hierarchy. As the US adopts an increasingly indirect approach to European security, Washington will devote fewer resources and attention to the achievement of its strategic objectives there. Three challenges stand out: ensuring that Russia and Germany do not become either too strong or too weak, ensuring that the Russian-German relationship is neither too cooperative nor too conflictual, and empowering key allies in Western Europe (notably Britain and France) and helping them preserve a regional balance of power. Below, we address each of these challenges in turn.

Preserving a Favorable European Balance: Neither Too Strong nor Too Weak

To preserve the European balance, the US has long sought to ensure that Germany and Russia are neither too strong nor too weak. While German power is comfortably anchored in the institutional architecture of the current international order and a broader "transatlantic orientation," excessive German power in relation to the rest of Europe remains a concern noted by actors ranging from Trump's trade advisor Peter Navarro to the leader of the German Social Democratic Party.[52] Rising power in both Germany and Russia could lead to mutual apprehension and increase the risk of tensions. On the other hand, weakness in one could excessively embolden the other, which would risk disturbing the regional balance.[53] Either development could draw the US into unwanted and costly confrontation in Europe. Its increasing focus on the balance of

power in Asia constrains its flexibility and footprint to manage these less pressing risks in Europe.[54]

For one thing, growing Russian assertiveness militates against significant US disengagement from European geopolitics. Since the annexation of Crimea in 2014, Moscow's push to reestablish a sphere of influence in Eastern Europe has even led some observers to warn of an emerging "New Cold War" in Europe.[55] While there is vibrant debate about how durable Russian power may be, previous US administrations have considered Russia to be severely constrained by structural, economic, and demographic problems.[56] Furthermore, the presence of NATO and the EU along its western border, growing Chinese influence across Central Asia and Siberia, and ongoing instability in the Middle East have led Moscow to spread its resources across several fronts, limiting its ability to meaningfully threaten the European balance of power.[57] Yet Washington currently sees Russian aggression as a real risk and believes that credibly deterring Russia—and, critically, reassuring regional allies—requires some form of US military presence in Europe. In fact, since Russia's annexation of Crimea in 2014, the US has reinforced its military posture on the Continent. At the same time, its prioritization of China has led the United States to reassess the relative importance of certain subregions within Europe. It has constrained its engagement in areas like the Western Balkans, Ukraine, and the Caucasus while prioritizing the Baltic and Black Sea areas.[58]

Additionally, Germany has become, since the end of the Cold War, the economic and financial leader of the EU. Reunification and the enlargement of NATO and the EU to Eastern Europe brought additional security, autonomy, and economic opportunities for Berlin, reducing its strategic dependence on the US and NATO and even reinforcing its position vis-à-vis France and Britain.[59] Germany's centrality to the EU's response to the 2008 global financial crisis and in EU policy toward Russia since 2014 illustrate its rise.[60] But the need to negotiate decisions with multiple partners and institutions in the context of the EU still constrains Germany as well. France and the UK (perhaps less so after Brexit) also remain important political counterweights to German leadership within Europe. Moreover, while Germany has taken on a stronger leadership role in European foreign policy in recent years on the diplomatic front, the German electorate's discomfort with military force limits the country's ability to play a leading security role.[61]

In contrast to previous US administrations, however, the Trump administration did not think of the EU as a constraint on Berlin. Instead, it saw the EU as a mechanism to further German interests and power and even

supported anti-EU initiatives and movements, including Brexit.[62] This approach is not purely ideological: Washington faces a long-standing dilemma with regard to European integration.[63] To the extent that European integration promotes political cooperation, stimulates economic growth, and helps balance Russian power while harnessing German power, it is positive for US interests. However, if the EU were to become either too strong or dominated by a single power, US interests in European balance would be at risk.[64] Washington's attitude toward defense cooperation in an EU framework is a good example: the United States welcomes EU efforts aimed at strengthening defense capabilities as positive contributions to the transatlantic security relationship.[65] However, it is suspicious about attempts in the EU to develop an exclusive approach toward defense policy both on industrial and geostrategic grounds, as it could prove harmful to the position of US defense companies on the European market while constraining US leadership in the transatlantic community.[66]

While the prospect of a politically and strategically integrated Europe is not exclusively dependent on Germany, Berlin's active participation and leadership (in cooperation with France) is indispensable for any real breakthrough in that regard. That means that German power and the specter of a strategically and politically united Europe are two interrelated challenges for US grand strategy.[67] In this regard, as Washington rebalances its attention toward China and the Indo-Pacific, ensuring that the European integration process does not decouple from the wider transatlantic framework and advance in a direction harmful to US interests promises to become increasingly challenging.

Balancing between Intra-European Cooperation and Conflict

The US has traditionally sought to ensure that the relationship between Germany and Russia is neither too cooperative nor too conflictual. This is the case because too much German-Russian cooperation could lead to some form of condominium between the two and upset the European balance, thereby undermining US regional influence and freedom of action.[68] A key illustration of this dynamic is US opposition to the construction of Nord Stream 2, a 1,200-kilometer-long offshore natural gas pipeline between Russia and Germany. US officials accuse Berlin of ignoring the interests of its allies by filling Russia's coffers and bypassing Central and Eastern European countries, leaving them vulnerable to Russian pressure.[69] They fear that Nord Stream 2 would allow Moscow to threaten credibly to cut off gas supplies in Eastern Europe without undermining its business with Western Europe.[70] Because Nord Stream 2 would make Germany the

key transit country in continental Europe, critics have accused Berlin of profiting at the expense of its neighbors, who would find themselves paying more at the end of the transport route through Germany.[71] Chancellor Merkel's government continues to defend the project as a purely commercial initiative, however, if less energetically following pressure from allies resulting from the poisoning of Russian dissident Alexei Navalny.

Even as US policy makers are wary of a cooperative German-Russian relationship, conflict in Europe is an entanglement risk that the US would prefer to avoid.[72] If anything, this dilemma is likely to become more salient as the US strives to keep its engagement in Europe relatively contained. Thus, as Washington continues to shift its attention toward China and the Indo-Pacific, it will likely seek engagement in Europe that is sufficient to influence the strategic interaction between Germany and Russia. Such proactive engagement in Europe, even if somewhat costly, may prove to be an effective insurance policy against costlier risks.

Keeping a Strong Anchor in Western Europe

Finally, the existence of strong and independent countries in Western Europe firmly allied with the United States geopolitically has historically given Washington strategic reach in the region. In particular, a strong alliance with nuclear powers Britain and France is key from a US perspective, as their strategic autonomy supports a European balance of power. During the Second World War, Britain's ability to withstand an invasion was essential to the logistics supporting Europe's liberation. During the Cold War, the UK and France played important roles in both nuclear and conventional deterrence. Both remain today an important buffer against the specter of German economic and diplomatic dominance in Europe.[73] Critically, their status as Europe's most capable conventional and only nuclear powers allows France and the UK to guide Germany in security matters while also deterring Russia.

If anything, the importance of France and the UK, and their role in managing German and Russian power in Europe, is likely to increase as the US shifts its focus to Asia. At the same time, the 2011 Libya intervention highlighted that British and French influence in and around Europe is more effective with US support. Thus, as it prioritizes China and the Indo-Pacific, the United States may strive to find a balance between delegating greater responsibility to Britain and France in Europe and ensuring a sufficient level of engagement to support those two countries. For example, France leans on the United States to balance resources required to manage terrorism-related challenges in the Sahel while also supporting

NATO efforts to deter Russia and defend the Baltic States. Yet resource constraints and a potentially unbalanced Europe are no longer the only challenge for America's European strategy. An increasingly important challenge relates to ensuring that Europe's key actors and institutions support—or at least do not hinder—US efforts in the context of its competition with China.

The US-China Rivalry: Coordinating with Europe

It has become rather commonplace in US scholarly circles to assert that Europe's global importance is decreasing. Experts in grand strategy are less and less interested in Europe-related developments, while China and Asia experts are increasingly in demand.[74] Nevertheless, the European continent is not immune from Sino-American competition. In fact, in (re) framing its European strategy, Washington has started to think beyond its traditional concern with preserving a regional balance of power and seeks to ensure that Europe's key powers and institutions are on its side when it comes to competition with Beijing. This important consideration is increasingly affecting how the United States interacts with its European allies and competitors.

America's European Allies and Competition with China

The relationship between Washington's European partners and its competition with China is largely technological and economic. Current efforts by Chinese state-led companies to access—and eventually dominate—global markets in key technologies like 5G and AI raise important strategic as well as privacy- and competition-related issues. China's disinterest in Western standards, coupled with lack of reciprocity and other barriers to foreign companies operating in the Chinese market, makes these challenges even more acute. The lack of a level playing field ultimately means that China could leverage global supply chains and infrastructure nodes to game the current international order against American power. Europe's advanced economies are an important prize in that context.

Against this background, several Trump administration officials warned Europeans that using technology from Chinese telecommunications manufacturer Huawei could hurt their relationship with the United States. Washington accused Huawei of being a Trojan horse for Chinese intelligence and has tried to check its influence.[75] Nonetheless, most Europeans appear to believe that the security risks are manageable, proposing additional security requirements rather than a complete ban.[76] In response,

Washington warned that the inclusion of Huawei equipment in next-generation mobile networks could curtain intelligence sharing and hurt relations with the US.[77] It also announced sanctions to those foreign tech manufacturers that sell computer chips built with American technology to Huawei.[78] Although there was some domestic criticism of Trump's transactionalist approach to the issue, a bipartisan effort is underway to stimulate smaller non-Chinese companies to make individual pieces of networking equipment that interact with one another, breaking Huawei's market dominance.[79] This effort further underlines the United States' preoccupation with the prospect of Chinese dominance in this field. And in any case, dependence on Chinese 5G solutions would make Europeans vulnerable to Chinese sabotage of different sorts.

Beyond 5G, which has become a particularly contentious issue in transatlantic relations as of late, Washington is increasingly worried about China's growing economic and political influence across Europe.[80] One concern is the 16+1 (17+1 since the formal inclusion of Greece in April 2019), a forum involving China and a number of Central and Eastern European countries to discuss issues relating to investment, economic, and trade cooperation. After the launch of the Belt and Road Initiative (BRI) in 2013, the 17+1 format turned into a platform for China to develop infrastructure projects to connect China to Europe. It aimed to facilitate Chinese access to European markets and export its excess capital and labor while building its economic reach on the Continent.[81] The 17+1 format has allowed China to bypass the EU as a bloc and strengthen its diplomatic and political influence over individual countries. For instance, when Hungary broke the EU's consensus on human rights violations in March 2017 by refusing to sign a joint letter denouncing China's alleged torture of detained lawyers, some observers were quick to link this to increased Chinese investment in the country.[82] Similar reactions emerged in July 2016, when Hungary and Greece blocked a reference to Beijing in a Brussels statement on the illegality of Chinese claims in the South China Sea.[83]

Over the past decade, the economic and migration crises have exacerbated several cleavages within and between European countries, among which the North-South and East-West divides stand out. As the 17+1 platform illustrates, China has proven quite adept at drawing on those divisions while leveraging its financial and economic largesse to increase economic presence and political influence in Europe.[84] This strategy has caused alarm in the United States. In a 2018 speech at the Heritage Foundation, former assistant secretary of state for European affairs A. Wess Mitchell alluded to parts of Europe as a new playground for China.[85] Relatedly, ac-

cording to a senior White House official, "China poses an even greater threat to Europe than Russia does" because Russia's interests and behavior in the old continent are "relatively predictable," whereas China's are unpredictable, making China "a highly disruptive force in Europe."[86] Russia's economic weakness and thirst for European capital empower European countries vis-à-vis Moscow, opening up the possibility of employing sanctions and other tools of economic statecraft. Yet it is unclear to what extent Europeans are able or willing to adopt similar strategies with Beijing.

The United States is concerned about China's growing economic and political influence *within* Europe for two reasons. First, it enables China to amass European financial or market access support for its bid to dominate key technologies such as 5G, neutralizing potential European support for the United States in the context of its long-term strategic competition with Beijing, or even allowing Beijing to gather support in some instances. Second, China's ability to engage with European countries bilaterally or through subregional clusters challenges European cohesion. The 17+1 framework is particularly striking, as it encroaches into core EU competences like trade or infrastructure. Traditionally, US policy makers have viewed European cohesion as an important enabler of US power. Since sowing divisions and instability is cheaper for China than it is for the United States and its European allies to redress such divisions, China's policies are deemed problematic. Admittedly, the Trump administration has departed from the long-standing American tendency to consider European cohesion as an end of US strategy.[87] Nonetheless, US leadership considers a Europe divided on Chinese terms a risk for Washington.[88]

Beyond China's influence, Europe's place in Sino-American competition is also about how Europeans may facilitate or hinder Chinese influence in other regions, most notably along the Indo-Pacific maritime axis.[89] Some US officials expect European allies to play a more proactive role in the Indo-Pacific, stepping up their diplomatic and military presence there and joining forces with Washington and its Asian allies, including in territorial disputes with China.[90] Former US secretary of defense Leon Panetta, in his farewell speech in Europe, urged US European allies to accompany Washington as it rebalanced its strategic attention to Asia.[91] At the same time, Russia's annexation of Crimea and the decision to strengthen deterrence in Eastern Europe may be affecting America's calculus, as facing two "long-term strategic competitors" (China and Russia) and a constrained resource environment forces the United States to prioritize. Against this backdrop, there is a growing feeling amid US defense officials that the most efficient way to use the resources and capabilities of

US European allies is to deter Russia and provide security in their own continent (and its immediate neighborhood), thus (partly) relieving Washington of its burden there as it prioritizes Asia and the Indo-Pacific.[92] In the words of one US defense official, European allies "should focus on holding the line in Eastern Europe" and let "the United States and its East Asian allies guarantee security in Asia and the Indo-Pacific."[93] At the same time, however, US policy makers also realize that Europeans have their own interests in Asia and the Indo-Pacific. Thus, a key challenge for the United States going forward is how to steer the activities of its European allies in the Indo-Pacific in a fruitful direction from the viewpoint of its competition with China.

How could Washington's European allies assist the US in its competition with China in the primary Indo-Pacific front, contributing to a favorable balance of power there? One important challenge is ensuring that European technology does not fuel China's military modernization. For several decades, Washington has exerted considerable pressure on the EU to maintain its arms embargo against the PRC, even threatening adverse consequences for transatlantic defense industrial relations.[94] As competition with China becomes more salient, the United States is also paying increasing attention to Europe's transfer of "dual-use" technology to China and has urged some of its allies (in particular the French) to scrutinize more carefully their technology and capability transfers to China.[95]

Beyond the issue of arms transfers, the United States is devoting increasing attention to the security role that countries like Britain or France can play across the Indo-Pacific, as both possess an important infrastructure of overseas bases across the region, powerful navies, and growing strategic ties with key US allies and partners in the region.[96] Thus, Washington is encouraging greater military-to-military interaction with Britain and France in the Indo-Pacific as well as supporting greater connectivity between those two countries and its key allies and partners in the Indo-Pacific. Finally, the United States is worried about European signs of support to Chinese efforts to reorder Asia and the Indo-Pacific region in its favor. In this regard, in 2015, Britain, Germany, France, and Italy decided to join the Chinese-led Asian Infrastructure Investment Bank (AIIB), ignoring pleas from the Obama administration not to do so.[97] To manage this problem, the United States has recently sought to elevate the question of China and the US-China competition to the top of the transatlantic political agenda, as illustrated by the summit of NATO heads of state and government in Washington, DC, in April 2019 and the leaders' meeting in November 2019.[98]

Competition with China and the Future of US-Russia Relations

The China factor will also become increasingly important in US strategic calculations vis-à-vis Russia. The growing Sino-Russian relationship poses a significant challenge for the US—while it will certainly seek to avoid a China-Russia alignment, it is unlikely that the US would align with either against the other in the current environment, as some have argued. Russia's connection to Asia and to the broader process of Sino-American competition is perhaps clearer than that of other European states. It is through Russia that the connections between the European and Asian theaters become most apparent. Russian fears about China's growing influence in Central Asia, Eastern Siberia, or even the Arctic could offer an opportunity for a US-Russia rapprochement—analogous to the US opening to China during the Cold War, which forced the USSR to divide its attention and resources across Europe and Asia. In this regard, Richard Betts argues that since "the rise of China is ultimately a more serious security challenge than Russian reassertion . . . realists should hope for a way to achieve a US rapprochement with Russia."[99] Nevertheless, Putin's regime identifies the United States as the main threat to its security, and Russia has made its relationship with China a strategic and geo-economic priority. Their 1997 border agreement, coupled with both countries' seeming determination to sooth existing frictions, has ensured an amicable relationship in recent years, enabling both parties to focus on competition with the US. From a US viewpoint, a hostile Russia can cause mischief but remains "weak and sufferable."[100] Russia and China together, however, are a much tougher challenge.

From a Russian viewpoint, the more Moscow signals to Washington that its relationship with Beijing is strong, the higher the price the US may be willing to pay politically to pry Russia away from China. US officials are by and large skeptical of America's ability to manipulate the Sino-Russian relationship. However, there is a growing recognition in Washington that an excessively confrontational approach toward Russia in Europe could push Moscow closer to Beijing, compromising America's broader geopolitical standing.[101] This scenario creates an important dilemma for the United States, as Russia could conclude that touting its strategic ties with China could help extract geopolitical concessions from the US.[102] Yet as Washington prioritizes its competition with Beijing, preventing the consolidation of a Sino-Russian bloc becomes important. Should, then, the US accept Russian interests in Europe or the Middle East in exchange for Russia's cooperation in limiting Chinese influence in regions like Central Asia, the Arctic, or the Western Pacific or even Russian

neutrality in Asian geopolitics? More broadly, what can Russia do for or against the US in Asia and in relation to China more specifically?

There are already signs suggesting that China and Asia may be increasingly relevant to US-Russia relations. Analysts have argued that the US decision to withdraw from the bilateral Intermediate-Range Nuclear Forces Treaty (INF) with Russia followed a realization that Beijing (which was not part of the treaty) was making gains at the expense of both Washington and Moscow.[103] Despite official insistence that European security concerns drove the decision to suspend its obligations under the INF, many experts have argued that the decision was actually driven by a desire to develop and deploy systems prohibited under the INF to counter Chinese capabilities. Since Beijing is no party to the arms control treaty, US officials have argued that the People's Liberation Army has an advantage there.[104] This raises an important question: Is the United States willing to embrace decisions that might be detrimental to the security of its European allies and interests for the sake of the higher-order objective of outcompeting China?

In the short term, however, three factors are likely to complicate US-Russia rapprochement. First, the US electorate remains suspicious of Russia—investigations of Russian influence in the 2016 US presidential election remain salient. Second, alliances in Europe still shape US behavior, and Russia poses an immediate threat to some US regional allies. Finally, Russia's behavior challenges American values as well as US security interests in Europe. As a matter of fact, both Republicans and Democrats are generally reluctant to accommodate Russia for the sake of balancing against China and deeply mistrust Moscow. The combination of the above factors complicates fundamental change. Nonetheless, as Washington looks at Russia through both a European and an Asian lens, and through the specific lens of the Sino-American competition, a delicate balancing act lies ahead.

Conclusion

Competition with China has become the United States' top grand strategic priority. In examining how Sino-American competition, both in Asia and globally, affects the US European strategy, we identified two sets of challenges for Washington going forward. The first relates to resource trade-offs and the evolving Europe versus Asia hierarchy in US grand strategy. Because resources are scarce and US strategy prioritizes competition with China, Washington will have fewer resources for a proactive role in Europe, enabling other actors (Germany, Russia, Britain, France, and

the EU) to increase their influence. The US is increasingly weighting its prioritization of the Indo-Pacific against the need to stay engaged in Europe, with a view to preserving a favorable regional balance of power. Going forward, US engagement will likely seek to prevent Germany, the EU, and Russia from becoming either too strong or too weak; to ensure that the relationship between those three actors is neither too cooperative nor too conflictual; and to enable Britain and France to remain strong enough to help Washington preserve a regional balance of power.

The second set of challenges relates to the United States expanding its traditional concern with preserving the European balance of power. It now also wants to be assured that Europe's key powers and institutions are on its side regarding competition with Beijing—or at least that they do not hinder US strategic objectives in terms of China and Asia. Toward this end, US strategy challenges that lie ahead in Europe include ensuring that European allies do not enable Chinese superiority in key technologies (including 5G or AI), ensuring that European activities in the Indo-Pacific support US strategic objectives, countering Chinese attempts to create division in Europe, and preventing Russia from becoming too close to China.

These conclusions have important implications for future research and policy analysis. We have based them on a simple premise: the prioritization of competition with China makes Europe a secondary theater for US grand strategy. We surely acknowledge that, when it comes to US China policy, different administrations will aim to strike their own balance between cooperation and competition and may thus make different choices regarding specific policies. However, there appears to be a broad consensus within the United States that competition with China is a structural phenomenon and is likely to be the key strategic challenge for Washington in the coming years or even decades. Against that backdrop, it is important for scholars to start thinking about what a China-first strategy means for US strategy elsewhere. Herein, we have sought to open that discussion through an analysis of America's European strategy.

Our analysis also has policy implications for the United States and Europe. We have outlined the broad contours of what Europe as a secondary theater means for US strategy on that continent. In particular, we have outlined the importance of reconciling the pressure on the US to downsize in Europe to focus on the Indo-Pacific with the need to maintain sufficient engagement to preserve a favorable regional balance of power in Europe. What kind of military posture, diplomatic strategy, or economic presence would that reconciliation require? We have barely scratched the surface of

that discussion, which is likely to remain key for US policy makers and scholars in the years to come. For their part, Europeans still need to come to terms with the notion that Sino-American competition may well become the ordering principle of international politics. As they do, they must also ascertain how they will position themselves in that context: Will they pick a side or, instead, emphasize European strategic autonomy and reject the frame of Sino-American competition? Experts and policy makers have only just begun to debate this question.[105] Their answers may well determine the shape and relevance of the transatlantic relationship in the twenty-first century. SSQ

Luis Simón

Dr. Simón is head of international security at the Institute for European Studies (Vrije Universiteit Brussel) and director of the Brussels office of the Elcano Royal Institute. He is also a member of the editorial board of the US Army War College's quarterly journal *Parameters*. Dr. Simón received his PhD from the University of London and held a postdoctoral fellowship at the Saltzman Institute for War and Peace Studies (Columbia University). His research has appeared in such journals as *Security Studies*, *International Affairs*, *The Journal of Strategic Studies*, *Geopolitics*, *Survival*, and *The RUSI Journal*. Contact him at luis.simon@vub.be.

Linde Desmaele

Linde Desmaele is a doctoral fellow at the Institute for European Studies at the Vrije Universiteit Brussel. She holds a master's degree from Seoul National University and from the Katholieke Universiteit Leuven (KU Leuven).

LTC Jordan Becker, USA

LTC Becker is currently the US liaison to the French Joint Staff. He was previously a senior transatlantic fellow at the Institute for European Studies, Vrije Universiteit Brussel, and completed his PhD at King's College London in 2017. Colonel Becker served as defense policy advisor to the US ambassador to NATO and as military assistant to the chairman of the NATO Military Committee (international military staff).

Acknowledgements

For their useful and constructive feedback, the authors would like to thank Daniel Fiott, Tongfi Kim, Alexander Lanoszka, Hugo Meijer, and Diego Ruiz Palmer.

Notes

1. For an overview of the progressive reorientation of US foreign policy attention toward Asia, see Nina Silove, "The Pivot before the Pivot: US Strategy to Preserve the Power Balance in Asia," *International Security* 40, no. 4 (2016): 45–88. https://doi.org/10.1162/ISEC_a_00238.

2. Department of State, "Deputy Secretary Zoellick Statement on Conclusion of the Second U.S.-China Senior Dialogue," 8 December 2005, https://2001-2009.state.gov/.

3. The White House, *National Security Strategy of the United States of America* (Washington, DC: Executive Office of the President, 2017), 2, 27, https://www.whitehouse.gov/.

4. Matthew Kroenig, *The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the US and China* (New York: Oxford University Press, 2020).

5. Aaron L. Friedberg, "Competing with China," *Survival* 60, no. 3 (2018): 7–64, https://doi.org/10.1080/00396338.2018.1470755; Dean P. Chen, "The Trump Administration's One-China Policy: Tilting toward Taiwan in an Era of US-PRC Rivalry?," *Asian Politics & Policy* 11, no. 2 (2019): 250–78, https://doi.org/10.1111/aspp.12455; and Kurt M. Campbell and Ely Ratner, "The China Reckoning: How Beijing Defied American Expectations," *Foreign Affairs* 97, no. 2 (March/April 2018), https://www.foreignaffairs.com/.

6. Evan Medeiros, "The Changing Fundamentals of US-China Relations," *The Washington Quarterly* 42, no. 3 (2019): 93–119, https://doi.org/10.1080/0163660X.2019.1666355.

7. Democratic Party Platform Committee, "2020 Democratic Party Platform," 27 July 2020, https://www.demconvention.com/.

8. We define *grand strategy* as the logic connecting a state's different elements of statecraft to its highest national objectives. See, for example, Christopher Layne, "Rethinking American Grand Strategy: Hegemony or Balance of Power in the Twenty-First Century?," *World Politics Journal* 15, no. 2 (1998): 8–28, https://www.jstor.org/stable/40209580.

9. Zak Doffman, "U.S. Threatens U.K. on Huawei and Intelligence Sharing," *Forbes*, 29 April 2019, https://www.forbes.com/.

10. Joseph Nye, "Is the American Century Over?," *Political Science Quarterly* 130, no. 3 (2015): 393–400, https://doi.org/10.1002/polq.12394; Michael Beckley, *Unrivaled: Why America Will Remain the World's Sole Superpower* (Ithaca: Cornell University Press, 2018); Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43, no. 3 (Winter 2018/19): 141–89, https://doi.org/10.1162/isec_a_00337; and Gordon G. Chang, *The Coming Collapse of China* (New York: Random House, 2010).

11. Silove, "The Pivot before the Pivot"; and Kai Liao, "The Pentagon and the Pivot," *Survival: Global Politics and Strategy* 55, no. 3 (2013): 95–114, https://doi.org/10.1080/00396338.2013.802855.

12. Hal Brands and Zack Cooper, "After the Responsible Stakeholder, What? Debating America's China Strategy," *Texas National Security Review* 2, no. 2 (2019), http://dx.doi.org/10.26153/tsw/1943; Hillary Clinton, "America's Pacific Century," *Foreign Policy*, 11 October 2011, https://foreignpolicy.com/; and Kurt Campbell, *The Pivot: The Future of American Statecraft in Asia* (New York: Basic Books, 2016).

13. Brands and Cooper, "After the Responsible Stakeholder."

14. The White House, *National Security Strategy,* 2, 26.

15. Department of Defense, *Summary of the 2018 National Defense Strategy: Sharpening America's Competitive Edge* (Washington, DC: Department of Defense, 2018), 1, 4, https://dod.defense.gov/.

16. The White House, *National Security Strategy,* 25.

17. Department of Defense, *Summary of the 2018 National Defense Strategy*, 4.

18. The White House, *National Security Strategy*; "Remarks by Vice President Pence on the Administration's Policy Towards China," Hudson Institute, Washington, DC, 4 October 2018, https://www.hudson.org/; Jansen Tham, "Why 5G Is the Next Front of US-China Competition," *The Diplomat*, 13 December 2018, https://thediplomat.com/;

and Ryan Hass and Zach Balin, "US-China Relations in the Age of Artificial Intelligence," Brookings (blog), 10 January 2019, https://www.brookings.edu/.

19. "Remarks by Vice President Pence."

20. Michael C. Horowitz, "Artificial Intelligence, International Competition and the Balance of Power," *Texas National Security Review* 1, no. 3 (2018), https://doi.org/10.15781/T2639KP49.

21. The White House, *National Security Strategy*; and Department of Defense, *Summary of the 2018 National Defense Strategy*.

22. Peter Dombrowski and Simon Reich, "Does Donald Trump Have a Grand Strategy?," *International Affairs* 93, no. 5 (2017): 1013–1037, https://doi.org/10.1093/ia/iix161.

23. Donald J. Trump, *Crippled America: How to Make America Great Again* (New York: Simon and Schuster, 2015); and "Remarks by Vice President Pence."

24. Michael R. Pompeo, "Interview with Hugh Hewitt of the Hugh Hewitt Show," transcript, 10 December 2018, https://www.state.gov/.

25. Aahron Mehta, "In Testimony, Shanahan Underlines It's 'China, China, China,'" *Defense News*, 14 March 2019, https://www.defensenews.com/.

26. Authors' interviews with multiple US defense officials in Washington, DC, and Brussels, September 2018–October 2019. See also Elbridge Colby et al., "Ready to Compete? America's Military and Technological Edge," War on the Rocks Podcast, 4 February 2019, https://warontherocks.com/.

27. Senior US defense official, authors' interview, Washington, DC, 22 October 2018.

28. Brands and Cooper, "After the Responsible Stakeholder"; David Dollar, Ryan Hass, and Jeffrey A. Bader, "Assessing US-China Relations 2 Years into the Trump Presidency," Brookings Institution, 15 January 2019, https://www.brookings.edu/.

29. Barbara Starr, "US Navy Proposing Major Show of Force to Warn China," CNN, 4 October 2018, https://edition.cnn.com/.

30. Joseph R. Biden Jr., "Why America Must Lead Again: Rescuing U.S. Foreign Policy after Trump," *Foreign Affairs* (March/April 2020): 64, https://www.foreignaffairs.com/; "The Power of America's Example: The Biden Plan for Leading the Democratic World to Meet the Challenges of the 21st Century," Biden/Harris presidential campaign page, 2021, http://joebiden.com/; and Democratic Party Platform Committee, "2020 Democratic Party Platform."

31. Department of Defense, *Summary of the 2018 National Defense Strategy*, 4.

32. Department of Defense, 4; and The White House, *National Security Strategy,* 47–50.

33. The White House, *National Security Strategy,* 47.

34. Orville Schell and Susan L. Shirk, *Course Correction: Toward an Effective and Sustainable China Policy* (New York: Asia Society Center on U.S.-China Relations, February 2019), https://asiasociety.org/.

35. Nicholas J. Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New Jersey: Transaction Publishers, 1942). We exclude the Middle East from our analysis even though it has long been a priority for the US because of energy geopolitics and it is within the framework of the war on terrorism. However, two fundamental factors make the Middle East less central to US grand strategy than Europe and (East) Asia. First, political instability and limited military-industrial potential (beyond resource extraction) limit regional powers' ability to project power beyond the

Middle East, let alone as far as the Western Hemisphere. Second, several middle regional powers have precluded the rise of a regional hegemon that could plausibly do so.

36. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton & Company, 2001).

37. Spykman, *America's Strategy in World Politics.*

38. Melvyn P. Leffler, *A Preponderance of Power: National Security, the Truman Administration, and the Cold War* (Palo Alto: Stanford University Press, 1992); Robert Ross, "US Grand Strategy, the Rise of China, and US National Security Strategy for East Asia," *Strategic Studies Quarterly* 7, no. 2 (2013): 20–40, https://www.airuniversity.af.edu/; and Stephen G. Brooks and William C. Wolforth, *America Abroad: Why the Sole Superpower Should Not Pull Back from the World* (Oxford: Oxford University Press, 2016).

39. Dean Acheson, Ernest Bevin, and Robert Schuman, "Communiqué on Germany (New York)," 19 September 1950, CVCE (Virtual Center for Knowledge about Europe), https://www.cvce.eu/.

40. Timothy Andrews Sayle, *Enduring Alliance: A History of NATO and the Postwar Global Order* (Ithaca, NY: Cornell University Press, 2019).

41. Wolfram F. Hanrieder, "Germany, the New Europe, and the Transatlantic Connection," *International Journal* 46, no. 3 (Summer 1991): 394–419, https://doi.org/10.2307/40202896; and Stanley R. Sloan, *Defense of the West: NATO, the European Union and the Transatlantic Bargain* (Manchester: Manchester University Press, 2016).

42. John L. Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War,* 2d ed. (New York: Oxford University Press, 2005).

43. Brooks and Wolforth, *America Abroad.*

44. John L. Gaddis, "A Grand Strategy of Transformation," *Foreign Policy,* no. 133 (November–December 2002): 50–57, https://doi.org/10.2307/3183557.

45. The White House, *National Security Strategy*; and Department of Defense, *Summary of the 2018 National Defense Strategy*, 48.

46. Christopher Layne, "This Time It's Real: The End of Unipolarity and the Pax Americana," *International Studies Quarterly* 56, no. 1 (2012): 203–13, http://www.jstor.org/stable/41409832.

47. G. John Ikenberry, "The Rise of China and the Future of the West: Can the Liberal System Survive?," *Foreign Affairs* 87, no. 1 (January–February 2008): 23, https://www.jstor.org/stable/20020265.

48. John J. Mearsheimer, "Bound to Fail? The Rise and Fall of the Liberal International Order," *International Security* 43, no. 4 (Spring 2019): 7–50, https://doi.org/10.1162/isec_a_00342.

49. Luis Simón, "Understanding US Retrenchment in Europe," *Survival* 57, no. 2 (2015): 157–72, https://doi.org/10.1080/00396338.2015.1026093.

50. The latter two are distinct but related because an independent EU would revolve either around German dominance or a strong Franco-German core.

51. Melvyn P. Leffler, "The Strategic Thinking That Made America Great: 'Europe First' and Why It Still Matters," *Foreign Affairs*, 10 August 2018, https://www.foreignaffairs.com/; and John R. Deni, "Pivot to Europe," *The National Interest*, 26 March 2014, https://nationalinterest.org/.

52. Jamie McGeever, "Trump Trade Adviser Says Germany Using 'Grossly Undervalued' Euro," Reuters, 31 January 2017, https://www.reuters.com/; and Martin Schultz and Thomas Oppermann, "SPD rechnet mit Verteidigungsministerin von der Leyen ab"

["SPD Settles with Defence Minister von der Leyern"], *Berliner Morgenpost*, 6 August 2017, https://www.morgenpost.de/.

53. Christopher Layne, "US Hegemony and the Perpetuation of NATO," *Journal of Strategic Studies* 23, no. 3 (2000): 59–91, https://doi.org/10.1080/01402390008437800.

54. Robert Powell, "Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate," *International Organization* 48, no. 2 (Spring 1994): 313–44, https://doi.org/10.1017/S0020818300028204.

55. Edward Lucas, *The New Cold War: Putin's Russia and the Threat to the West* (London: MacMillan, 2004); and Diego A. Ruiz Palmer, *Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs and Cold War Comparisons*, NDC Research Paper no. 120 (Rome: NATO Defence College, Research Division, October 2015), https://www.files.ethz.ch/.

56. Michael Kofman, "Russian Demographics and Power: Does the Kremlin Have a Long Game?" War on the Rocks, 4 February 2020, https://warontherocks.com/; Simon Saradzhyan and Abdullaev Nabi, "Measuring National Power: Is Putin's Russia in Decline?" *Europe-Asia Studies* (4 May 2020): 1–27, http://www.tandfonline.com; and Reuters, "Obama: 'Russia Doesn't Make Anything,' West Must Be Firm with China," 3 August 2014, https://www.reuters.com/.

57. Eugene B. Rumer and Celeste A. Wallander, "Russia: Power in Weakness," *Washington Quarterly* 27, no. 1 (2003): 57–73, https://ciaotest.cc.columbia.edu/.

58. US defense officials, interviews. See also Barry Pavel and Jeff Lightfoot, "The Transatlantic Bargain after 'The Pivot,' " *Atlantic Council Issue Brief,* 22 March 2012, https://www.atlanticcouncil.org/.

59. Hanrieder, "Germany, the New Europe, and the Transatlantic Connection"; and Hans Kundani, *The Paradox of German Power* (Oxford: Oxford University Press, 2015).

60. Ulrich Krotz and Richard Maher, "Europe's Crises and the EU's 'Big Three,' " *West European Politics* 39, no. 5 (2016): 1053–72, https://doi.org/10.1080/01402382.2016.1181872; and Simon Bulmer and Jonathan Joseph, "European Integration in Crisis? Of Supranational Integration, Hegemonic Projects and Domestic Politics," *European Journal of International Relations* 22, no. 4 (2016): 725–48, https://doi.org/10.1177/1354066115612558.

61. Beverly Crawford and Kim B. Olsen, "The Puzzle of Persistence and Power: Explaining Germany's Normative Foreign Policy," *German Politics* 26, no. 4 (2017): 591–608, https://doi.org/10.1080/09644008.2017.1364365.

62. Mike R. Pompeo, "Restoring the Role of the Nation-State in the Liberal International Order" (speech, German Marshall Fund, Brussels, 4 December 2018), https://www.state.gov/. See also Graham K. Wilson, "Brexit, Trump and the Special Relationship," *The British Journal of Politics and International Relations* 19, no. 3 (2017): 543–57, https://doi.org/10.1177/1369148117713719; Harold James, "Trump's Currency War Against Germany Could Destroy the EU," *Foreign Policy,* 2 February 2017, https://foreignpolicy.com/; and "Full Transcript of Interview with Donald Trump," *The Times*, 16 January 2017, https://www.thetimes.co.uk/.

63. Wyn Rees, "America, Brexit and the Security of Europe," *The British Journal of Politics and International Relations* 19, no. 3 (2017): 558–72, https://doi.org/10.1177/1369148117711400.

64. Layne, "US Hegemony and the Perpetuation of NATO."

65. Sven Biscop, "The Future of the Transatlantic Alliance: Not Without the European Union," *Strategic Studies Quarterly* 14, no. 3 (Fall 2020): 81, https://www.airuniversity.af.edu/; and remarks by Deputy US Assistant Secretary of State for Europe Matthew G. Boyse at a meeting organized by the Romanian EU Presidency in Bucharest, 17 April 2019.

66. Biscop, 81. See also Steven Erlanger, "US Revives Concerns about European Defence Plans, Rattling NATO Allies," *New York Times*, 18 February 2018, https://www.nytimes.com/.

67. US State Department official, authors' interview, Washington, DC, 23 October 2018.

68. Christopher S. Chivvis and Thomas Rid, "The Roots of Germany's Russia Policy," *Survival* 51, no. 2 (2009): 105–22, https://doi.org/10.1080/00396330902860850.

69. US defense officials, interviews. See also Antto Vihma and Mikael Wigell, "Unclear and Present Danger: Russia's Geoeconomics and the Nord Stream II Pipeline," *Global Affairs* 2, no. 4 (2016): 377–88, https://doi.org/10.1080/23340460.2016.1251073.

70. Georg Zachman, "Nord Stream 2: A Bad Deal for Germany and Eastern Europe," Bruegel, 18 July 2016, http://bruegel.org/.

71. Zachman, "Nord Stream 2"; and Vihma and Wigell, "Unclear and Present Danger."

72. Barry R. Posen, *Restraint: A New Foundation for U.S. Grand Strategy* (Ithaca, NY: Cornell University Press, 2014).

73. Insofar as mitigating German influence within the EU specifically, France is likely to become particularly important in a post-Brexit context. For an analysis of the Franco-German relationship, see Ulrich Krotz, "Three Eras and Possible Futures: A Long-Term View on the Franco-German Relationship a Century after the First World War," *International Affairs* 90, no. 2 (2014): 337–50, http://www.jstor.org/stable/24538558.

74. See, for example, Mearsheimer, "Bound to Fail?"; and Mike J. Green and Zack Cooper, "Revitalizing the Rebalance: How to Keep US Focus on Asia," *The Washington Quarterly* 37, no. 3 (2014): 25–46, https://doi.org/10.1080/0163660X.2014.978434.

75. Nigel Inkster, "The Huawei Affairs and China's Technology Ambitions," *Survival* 61, no. 1 (2019): 105–11, https://doi.org/10.1080/00396338.2019.1568041; and Alyza Sebenius, "U.S. Tries to Freeze Huawei out of Europe with Court Argument," Bloomberg, 9 April 2019, https://www.bloomberg.com/.

76. Gisela Grieger, European Parliament Research Service, "5G in the EU and Chinese Telecoms Suppliers," *At a Glance*, April 2019, http://www.europarl.europa.eu/.

77. Mike R. Pompeo, "Remarks at U.S. Embassy Budapest," 11 February 2019, https://hu.usembassy.gov/; Lucy Fisher and Mark Bridge, "Ban Huawei or Our Defence Links Will Suffer, US Warns," *The Times*, 11 April 2019, https://www.thetimes.co.uk/; and Yixiang Xu, "More Than a Choice between Huawei or US: The Cost for Europe's Pursuit of 5G," American Institute for Contemporary German Studies, 14 March 2019, https://www.aicgs.org/.

78. Janosch Delcker, "Privacy in the Pandemic Era—Germany's Huawei Headache—SPD Telenova, *Brussels Playbook*, Politico, 21 April 2020, https://www.politico.eu/.

79. David E. Sanger and David McCabe, "Huawei Is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives," *New York Times*, 17 February 2020, updated 14 July 2020, https://www.nytimes.com/.

80. See Philippe Le Corre and Alain Sepulchre, *China's Offensive in Europe* (Washington, DC: The Brookings Institution, 2016), https://www.brookings.edu/.

81. Investment and Development Agency of Latvia, "Meeting of China-CEEC Business Council and Business Support Organizations," Riga, Latvia, 20 June 2017, China IPR SME Helpdesk, https://www.china-iprhelpdesk.eu/.

82. Nick Cumming-Bruce and Somini Sengupta, "In Greece, China Finds an Ally against Human Rights Criticism," *New York Times*, 19 June 2017, https://www.nytimes.com/.

83. Georgi Gotev, "EU Unable to Adopt Statement Upholding South China Sea Ruling," EURACTIV, 14 July 2016, https://www.euractiv.com/.

84. US State Department official, interview.

85. A. Wess Mitchell, "The Transatlantic Bond: Preserving the West" (speech, The Heritage Foundation, Washington, DC, 2 October 2018), https://www.heritage.org/.

86. Senior White House official, authors' interview, Paris, 9 April 2019.

87. US State Department official, interview.

88. Mitchell, "The Transatlantic Bond."

89. Due to their economic, political, and security influence, Europeans can play an important role in hindering (or supporting) Chinese influence in regions like Africa, the Middle East, or Latin America. This is likely to become an increasingly important debate in the context of the transatlantic relationship, but space-related reasons preclude us from discussing that here.

90. US defense officials, interviews.

91. "Secretary Panetta's Remarks at King's College London," 18 January 2013, RealClearPolitics, https://www.realclearpolitics.com/.

92. US defense officials, interviews. See also Pavel and Lightfoot, "The Transatlantic Bargain."

93. Senior US defense official, interview.

94. Hugo Meijer et al., "Arming China: Major Powers' Arms Transfers to the People's Republic of China," *Journal of Strategic Studies* 41, no. 6 (2018): 850–86, https://doi.org/10.1080/01402390.2017.1288110.

95. US defense officials, interviews.

96. US defense officials, interviews. See also Erik Brattberg, Philippe Le Corre, and Etienne Soula, "Can France and the UK Pivot to the Pacific?," Carnegie Endowment for International Peace, 5 July 2018, https://carnegieendowment.org/; and Luis Simón, "Europe, the Rise of Asia and the Future of the Transatlantic Relationship," *International Affairs* 91, no. 5 (2015): 269–89, https://doi.org/10.1111/1468-2346.12393.

97. Andrew Higgins and David E. Sanger, "3 European Powers Say They Will Join China-Led Bank," *New York Times*, 17 March 2015, https://www.nytimes.com/.

98. Robbie Gramer, "Trump Wants NATO's Eyes on China," *Foreign Policy*, 20 March 2019, https://foreignpolicy.com/.

99. Richard K. Betts, "Realism Is an Attitude, Not a Doctrine," *The National Interest*, 24 August 2015, https://nationalinterest.org/.

100. Nadège Rolland, "A China-Russia Condominium over Eurasia," *Survival* 61, no. 1 (2019): 7–22, https://doi.org/10.1080/00396338.2019.1568043.

101. US defense officials, interviews. See also Andrea Kendall-Taylor and David Shullman, "A Russian-Chinese Partnership Is a Threat to U.S. Interests," *Foreign Affairs*, 14 May 2019, https://www.foreignaffairs.com/.

102. US State Department official, interview.

103. Scott A. Cuomo, "It's Time to Make a New Deal: Solving the INF Treaty's Strategic Liabilities to Achieve US Security Goals in Asia," *Texas National Security Review* 2, no. 1 (2018), http://dx.doi.org/10.26153/tsw/866; and Franz-Stefan Gady, "INF Withdrawal: Bolton's Tool to Shatter China-Russia Military Ties," *The Diplomat*, 24 October 2018, https://thediplomat.com/.

104. Alexander Lanoszka, "The INF Treaty: Pulling Out in Time," *Strategic Studies Quarterly* 13, no. 2 (2019): 48–67, https://www.airuniversity.af.edu/.

105. Luis Simón, "What Is Europe's Place in Sino-American Competition," War on the Rocks, 14 February 2019, https://warontherocks.com/; Sven Biscop, "1919–2019: How to Make Peace Last? European Strategy and the Future of the World Order," Egmont Institute, Security Policy Brief no. 102, 10 January 2019, https://www.egmontinstitute.be/; and Philippe Legrain, "The EU's China Conundrum," Project Syndicate, 5 April 2019, https://www.project-syndicate.org/.

PERSPECTIVE

An Interoperable Information Umbrella: Sharing Space Information Technology

Mariel Borowitz

Abstract

In 1996, Joseph Nye and William Owens foresaw the importance of information technologies and data sharing, warning that if the United States did not share the knowledge gained from its information systems—particularly satellites—other countries would have added incentive to develop their own. However, their analysis did not consider the potential benefits of resiliency offered by redundant allied systems. Decision makers should consider both the soft-power benefits of data sharing as well as the resiliency benefits associated with redundant, interoperable systems to enable a more robust path forward for gaining and preserving power in the information age. This article examines the disadvantages of restricting access to data as predicted by Nye and Owens and the unexpected benefits of redundancy for three space sector information technologies: reconnaissance satellites, global navigation satellite systems, and space domain awareness systems.

*****

In 1996, Joseph Nye and William Owens argued that the United States was poised to lead the information revolution, increasing its power in international affairs. Key to maintaining its technological superiority, however, was sharing this information. They recommended that the US provide an "information umbrella," sharing information to gain leverage with allies and maintain its leadership position. They noted that the United States has a considerable advantage in terms of investment and experience in these technologies and argued that if America did not share its knowledge it would create incentives for countries to develop independent capabilities. Conversely, its willingness to do so could be a way to build coalitions before aggression begins or to improve the decision-making of recipients during conflicts.[1]

Nye and Owens suggested that the US "information umbrella" should follow the model of the "nuclear umbrella." As with the nuclear umbrella, the information umbrella would provide leverage with allies and form the foundation for a mutually beneficial relationship. They acknowledged that this would require overcoming long-established prejudices against openly sharing intelligence. Concerns included the risks of disclosing sources and methods used in obtaining information and of making clear what the US did and did not know, potentially reducing its advantage. However, they concluded that "selectively sharing these abilities is therefore not only the route of coalition leadership, but the key to maintaining U.S. military superiority."[2]

The comparison to the nuclear umbrella provides a useful example to envision the potential benefits of information sharing, particularly space information, but the comparison is not perfect. While development of nuclear weapons is tightly restricted by the Treaty on the Non-Proliferation of Nuclear Weapons, there is no such restriction for space information technology. Nor are the dangers associated with the proliferation of this technology considered nearly as dire. This factor complicates the ability to develop and maintain an information umbrella but also broadens the policy options available. In many cases, the United States may find it beneficial to share data and encourage the development of independent space systems among allies.

James Clay Moltz states that "net-centric" space technology, based on resiliency gained through redundant systems and commercial and international partnerships, may be more critical in today's world than traditional views of power that emphasize purely national technologies. Further, Moltz contends that the United States is better situated than its potential adversaries to excel in this new form of power. The US has allies capable of developing and maintaining advanced space systems while its primary adversaries, Russia and China, have few, if any, close allies with this capability.[3] This suggests that combining information sharing and coordinated space technology development to enable more capable and resilient interoperable systems may provide greater security advantages than information sharing alone.

This article examines the historical development of three military space sector information technologies—reconnaissance satellites, global navigation satellite systems, and space domain awareness systems—and demonstrates that in these areas Nye and Owens's warning was prescient. The US reticence to engage in meaningful data sharing contributed to allies deciding to develop independent capabilities. However, the examined cases also

show that these developments resulted in unforeseen benefits to the United States in terms of redundancy and resilience that now play a critical role in US military power. These three cases indicate that the United States could have achieved benefits earlier, and with less tension among allies, if it had pursued a policy encouraging both information sharing and the development of interoperable systems. Lessons learned from these cases can be applied to future decision making.

Reconnaissance Satellites

The value of reconnaissance satellites has been evident since the beginning of the space age. The United States' first successful reconnaissance satellite mission, Corona, launched in 1960. This first satellite collected more imagery of the Soviet Union in two days than the U-2 reconnaissance aircraft had collected in two years of flights. Building on this success, the US reconnaissance program moved ahead rapidly, launching more than 100 reconnaissance satellites by 1972.[4]

Throughout this period, reconnaissance satellite technology and data were tightly controlled. When the US and the Soviet Union completed the first Strategic Arms Limitation Treaty in 1972, the agreement referred to verification by "national technical means." While this was understood by both parties to the treaty to refer to reconnaissance satellites, they deliberately chose not to publicly acknowledge the existence of these assets.[5] Even the presence of the United States National Reconnaissance Office (NRO), the agency that developed remote sensing satellites, remained classified until 1992.[6]

The United States' high level of secrecy and reluctance to share technology and data extended even to allies. In 1973, Israeli officials requested access to US reconnaissance imagery in support of the Yom Kippur War. US officials responded that the information was not available due to damage to the satellite. While this may have been true, Israeli officials were not convinced and chose to proceed with Israel's own satellite reconnaissance program.[7] Israel launched its first reconnaissance satellite, *Ofeq-1*, in 1988. This made Israel the fourth country in the world to develop a reconnaissance satellite, after the United States, the Soviet Union (1961), and China (1975).

The 1991 Persian Gulf War demonstrated continued limitations in US sharing of reconnaissance data with allies. In 1992, France requested US satellite imagery to support its efforts in the Gulf War. When the US declined to share the images, France started its own reconnaissance program.[8] France's first reconnaissance satellite, *Helios 1A*, was launched in 1995, fol-

lowed by increasingly capable satellites in the same series. France was the fifth nation to develop a reconnaissance satellite. The data from this series was used to support independent French decision-making. A French military official stated in 2015 that it was because of Helios imagery that France declined to join the 2003 US invasion of Iraq, as France's independent assessment of this imagery contradicted US interpretations of intelligence at the time.[9] See table 1 for inaugural satellite launch dates by country.

Table 1. Date of first reconnaissance satellite launch by country

Nation	First Reconnaissance Satellite
United States	1960
Soviet Union/Russia	1961
China	1975
Israel	1988
France	1995
Japan	2003
Germany	2006
India	2009
South Africa	2014
Turkey	2016
Italy	2017

While other factors, such as technical capability and prestige, likely impacted these decisions, US reticence to share its own reconnaissance data when requested also played a role in the Israeli and French development of independent reconnaissance satellite systems. Further, once these nations developed this technology, they were free to share the resulting information—or the technology itself—according to their own policies.

Unlike the US, France chose to undertake its satellite reconnaissance program as a cooperative effort. *Helios 1* was developed in partnership with Italy and Spain.[10] Later Helios satellites incorporated Greece and Belgium into the partnership. In 2006, Germany developed its own reconnaissance satellite system, SAR-Lupe, with a radar instrument allowing the collection of information regardless of weather and lighting conditions. A cooperative treaty with France allows both nations to access data from both the Helios and SAR-Lupe satellites.[11] France has a similar agreement in place for access to data from Italy's dual-use COSMO-SkyMed constellation, launched in 2007 and 2008, which also carries radar instruments.[12] In 2017, Italy launched its first dedicated reconnaissance satellite, built by Israel Aerospace Industries.[13]

In addition to the significant degree of data sharing among European nations, Israel, France, and others have also proven to be much more willing than the US to export advanced satellite remote sensing technology. Despite a multiyear process that began in 2009 to reform export control regulations, remote sensing systems with military applications remain on the tightly controlled United States Munitions List.[14] These systems include those with high spatial or spectral resolutions and many of those with radar remote-sensing characteristics, By contrast, allied nations spurred by the US to develop their own reconnaissance systems have shown a willingness to export this technology. In 2009, India launched its first reconnaissance satellite, the *Radar Imaging Satellite-2*, built by Israel Aerospace Industries. That same year, Turkey signed a contract with Thales Alenia Space of France and Italy's Telespazio to purchase a high-resolution imagery satellite, launched in 2016.

It is worth noting that, beginning in the 1980s, many countries—including the United States—promoted the growth of commercial remote-sensing companies capable of providing high-resolution imagery. The data sold by companies has proven valuable for national security and foreign policy uses.[15] However, these companies remain highly regulated. Limitations are placed on the spatial resolution of this imagery to ensure it remains less precise than data provided by advanced military reconnaissance systems. Companies are often prohibited from selling data in particular geographic areas, to particular customers, or at particular times.[16] While companies are regulated by the nation in which they reside, the US has also exerted "checkbook shutter control." That is, it purchases all available imagery under an exclusive license so no one else can access it. The US thus has a way of wielding some level of control even over foreign commercial systems. While some countries may find that their national security needs can be met solely through commercially available satellite data, the continued limitations on access and the differences in capability differentiate them from nationally owned reconnaissance satellites.

As Nye and Owens suggested, by failing to adequately share data, the US had created an additional incentive for allies to develop their own systems sooner than they may have otherwise. Once that development had occurred, the US ceded not only its leverage as a data provider but also control over further proliferation of both the information and the underlying technology.

Global Navigation Satellite Systems

Limited US data sharing also acted as an incentive for independent allied development of global navigation satellite systems. The US Department of Defense (DOD) launched the first experimental navigation satellite, *TRANSIT 1A*, in 1959. The system used measurements of the Doppler shift in the satellite signal to determine a receiver's location on Earth. The DOD planned to use the system to allow accurate positioning of submarines carrying Polaris missiles. The system was declared operational in 1964. A second system, Timation (time/navigation), experimented with spacecraft carrying precise clocks, with an initial launch in 1967. This project evolved into the Global Positioning System (GPS), established in 1973. By 1978, four GPS Block 1 satellites were operational. Although the constellation would not be considered operational globally until 24 satellites were in orbit (which occurred in 1993), the system proved to have utility early on.[17]

The Soviet Union engaged in the development of a parallel system, the Global Navigation Satellite System (GLONASS), with 10 satellites in orbit by 1985. The constellation became fully operational in 1996 but was not maintained; it included fewer than 10 operational satellites, on average, between 1998 and 2006. The system returned to full operational capacity in 2010.[18]

In 1983, a civilian aircraft, Korean Airlines 007, strayed into Soviet airspace and was shot down by a Soviet fighter jet. Following this incident, President Reagan announced that the GPS signal would be made available for civilian use. However, the civilian signal would be less precise than the military signal—accurate to approximately 100 meters versus 10 meters for the military. The US government would also have a capability referred to as "selective availability" that would allow the civilian signal to be deliberately degraded or disabled. Despite these restrictions, civilian GPS receivers were in mass production by the late 1980s.[19]

In a 1992 communication to the European Parliament, the European Commission noted that although the US military currently made the GPS signal freely available for civil use, this arrangement could be halted at any time. Further, the civilian signal's accuracy was insufficient for use in the civil air navigation system, a highly desirable application.[20] In 1994, a European Parliament resolution officially called for establishing a European strategy for satellite navigation, and the Commission responded with a proposal for an independent European global navigation satellite system.[21]

In response to this movement and recognizing the growing commercial industry built on GPS, President Bill Clinton issued a directive stating

that the United States was committed to providing the GPS signal "on a continuous, worldwide basis, free of direct user fees." The directive also stated that the US would discontinue the use of selective availability within a decade and that the government would advocate for the acceptance of GPS as the standard for international use.[22] This was too little, too late for Europe, which continued ahead with plans to develop its independent Galileo global navigation satellite system.

In 2001, US deputy secretary of defense Paul Wolfowitz sent a letter to the defense ministers in selected EU countries. He argued that the planned European system could complicate US plans to modify and improve GPS due to potential interference of the Galileo signal with the upgraded US military signal on GPS. He further indicated that the civilian forum in which Galileo was being developed was insufficient to fully assess the security implications of the system.[23]

European leaders did not respond well to this action. French president Jacques Chirac warned that Europeans risked "vassal status" if they abandoned the project. The European commissioner in charge of the project expressed frustration at "American pressure against the Galileo project" and the prospect of further delays.[24] The European Commission approved the next phase of development in 2002 and engaged in international cooperation, ensuring compatibility with the American GPS and Russian GLONASS systems. In 2016, the Galileo system reached initial operational status.[25] When Galileo becomes fully operational, it will be the fourth such constellation in the world, following the United States, Russia, and China. Once again, by refusing to make data available in a meaningful, reliable way, the United States added incentive for allies to create an independent system, and its efforts to dissuade such developments generated increasing tension.

Space Domain Awareness Systems

This pattern is being repeated once again for space situational awareness (SSA) systems—systems that track and analyze space objects to determine where they are, what they are, and where they are likely to be in the future.[26] The US has been tracking objects in space since the space age began with the 1957 launch of *Sputnik I*, and it has had an operational space surveillance system since 1958. The DOD worked with NASA, which also needed to track satellites, with both entities contributing observations to be cataloged by the DOD. In 1960, following the launch of the first Corona reconnaissance satellite, DOD officials determined that security concerns dictated withholding some data. The DOD began screening the catalog for

sensitive information before providing it to NASA, which then shared this information more broadly. This process, in which the DOD maintained a full tracking system while providing a subset of data to NASA for broader distribution, continued for more than 40 years.[27]

In 2001, the US government released the *Report of the Commission to Assess United States National Security, Space Management and Organization*—more commonly known as the Rumsfeld Report after the commission chairman, Secretary of Defense Donald Rumsfeld. The report recognized the significant and growing dependence of the US military and economy on space assets and noted that this made space assets potentially attractive targets for adversaries. The report warned of a "Space Pearl Harbor" and emphasized the need to improve SSA. Space situational awareness is critical to avoiding unintentional collisions among satellites and other debris in space and detecting and attributing attacks on space assets.[28]

In addition to the need for SSA data for military purposes, there was also a recognition that with the growth of commercial activity and increased civilian reliance on space assets, the US Air Force should provide warnings of threats to US or other friendly satellite operators. In 2000, a DOD memorandum directed the Air Force to study options for providing SSA support to commercial and foreign entities. The National Defense Authorization Act for Fiscal Year 2004 directed Air Force Space Command to implement a pilot program in this area.[29] The pilot program later became the operational SSA Sharing Program.

While the stated goal of the pilot program was to encourage international cooperation and transparency with foreign nations, the initial implementation fell short of expectations. The US Air Force maintained two catalogs—an internal high-accuracy catalog with detailed information on all tracked objects and the publicly accessible space track catalog with more basic information on a subset of space assets. The DOD routinely conducted conjunction analysis to determine the risk of a collision only for US military spacecraft, and the public catalog was inadequate to independently run this type of analysis. The limitations of this approach were demonstrated dramatically by the 2009 collision of an operational commercial Iridium communications satellite and a defunct Russian Cosmos satellite, which occurred with no advanced warning for Iridium operators.[30]

Following the Iridium-Cosmos collision, the US began running conjunction analysis for all operational satellites and contacting satellite operators in the event of a potential collision. However, initial efforts struggled to balance the desire to work with satellite operators with the need to protect sensitive data. One Air Force analyst described early efforts at assisting

operators in planning collision avoidance maneuvers as "kind of like playing 'Marco Polo.'"[31]

The US military has taken steps to substantially improve the situation since then. As of 2019, Strategic Command had signed agreements related to SSA services and data sharing with 19 nations; two international organizations; and more than 77 commercial satellite owners, operators, and launchers. These agreements allow higher-quality data to be shared more systematically.[32] The military has also begun increasing the amount of data made available through its public catalog.[33] Further, recent years have seen the emergence of commercial SSA entities, particularly in the United States, that sell SSA data and analysis to domestic and foreign satellite operators.[34]

However, there are still notable limitations to SSA data sharing. Even with recent improvements, the data provided in the public catalog remains insufficiently accurate to carry out conjunction analysis, and the US does not accept any liability for the information it shares.[35] Even when more accurate information or conjunction analyses are shared, the US does not provide insight into its data sources or algorithms, making it impossible for users to independently evaluate accuracy or conduct further analysis.[36]

The United States reserves the right to deny participants access to SSA data and information without prior notice or explanation. Participants in the SSA data-sharing program are restricted from redistributing the data without explicit approval from the US. Furthermore, users note that while the data is currently provided free of charge, the US government provides no guarantee that this will continue to be the case in the future. Outside of these specific limitations, some partners remain generally uncomfortable relying on a program run by the US military as it may have different priorities and concerns than foreign, commercial, and civil users.[37]

The slow development of data-sharing systems by the United States, combined with the continued limitations of those systems, has driven a number of allies to begin development of independent systems. In 2005, the European Commission convened a panel of space experts to report on security issues related to the European Space Policy. The group noted that while the United States was currently providing tracking data for free, "this situation could change in the near future, and the data already provided are not exhaustive or not be[ing] made available at the needed time." It recommended the development of a European space surveillance capability as a high-priority activity.[38] The European Commission announced in 2008 that it would develop this capability, emphasizing Europe's need

for political and technical autonomy.[39] In 2016, the European Union Space Surveillance Tracking system became operational.[40]

A 2018 report by the Institute for Defense Analysis identified a lack of confidence in DOD-provided data as a key driver for many foreign and commercial entities developing independent capabilities. In interviews, officials cited the lack of transparency related to DOD data, particularly the lack of insight into processing methods, as a key source of concern. Others called attention to issues of accuracy and completeness of the data provided. South Korean government officials estimated that their country was receiving data for about only 40 percent of objects tracked by the DOD. In addition to Europe and South Korea, India, Canada, Australia, and Japan are among those developing or improving national SSA capabilities.[41]

Unexpected Benefits: Redundancy and Improved Capabilities

In each of the above cases, the United States had an information advantage based on superior technology, just as Nye and Owens suggested. While the US did make some data available to allies, its efforts fell short of allies' needs and expectations. In all three cases, allies directly referenced the lack of US data sharing as a factor in developing independent systems. The US choice to limit the sharing of data—versus using data sharing to provide the basis of coalition leadership and to maintain technological superiority—led to tensions between the United States and its allies and contributed to allies' decisions to develop independent systems.

From Nye and Owens's perspective, this approach may be viewed as a strategic failure on the part of the United States. However, the development of independent allied systems has ultimately benefited the US. As US reliance on space assets has increased, their vulnerability has become a growing concern. The 2018 *National Defense Strategy* recognized that new threats to military and civil use of space were emerging and called for investments to prioritize efforts to assure space capabilities.[42] One of the widely agreed-upon methods for overcoming or deterring attacks on these assets is the development of redundant, resilient systems.

For example, given sufficient interoperability between the systems, if an adversary were to damage or disrupt GPS, the United States could switch to the Galileo signal. An attack on GPS would potentially have other ramifications, such as nuclear denotation detection, that would need to be dealt with in other ways. However, if the goal was to disable GPS, the ability to use Galileo should still be a deterrent. Knowing this, the adversary may determine that it is not worth attacking GPS in the first place. The same is true for redundant space reconnaissance and SSA systems.

From this perspective, allies' development of redundant military space systems may appreciably increase US national security. By engaging allies to build partnerships enabling the mutual sharing of information and technology, the US can reduce its vulnerability in these areas.

In addition to the benefits of resilience, cooperation and interoperability can improve performance. If the United States can negotiate gaining access to data from foreign reconnaissance systems, it will increase the volume of data available for analysis. Even without gaining regular access, the United States may reasonably assume that allies with mutual security concerns may be conducting surveillance and analysis with similar goals. Increasing the amount of data collected and the number of individuals and organizations analyzing this data reduces the risk that security threats will go undetected.

Coordinating navigation systems could be similarly beneficial. Receivers that can access the Galileo signal, in addition to GPS, will have more precise positioning capabilities. They will also be more likely to have access to a sufficient number of satellites for accurate positioning, even in rough terrain or urban canyons, and be more resistant to jamming or spoofing efforts. The United States and Europe have already begun to work toward this capability for military systems.

SSA technologies are primarily ground based, but the benefits of redundancy and improved performance are similar. The ability to accurately detect and attribute attacks on space assets, which relies on high-quality SSA data, is a crucial element in deterring such attacks. Just as for traditional reconnaissance data, the more space surveillance data that is collected and analyzed, the more likely it is that nefarious behavior will be detected and accurately attributed, thus improving deterrence.

While these examples focused on the military benefits of engaging allies in their development and operation of redundant systems, in the case of GPS and SSA, improved capabilities would also benefit civilian and commercial users of these systems.

Implications and Lessons Learned

Nye and Owens were not wrong when they recognized in 1996 that the nation able to lead in the information revolution would accrue power, and they correctly identified information sharing as an important source of leverage with allies. As was demonstrated in the cases of reconnaissance satellites, GPS, and SSA, they also correctly predicted that a lack of sharing would add an additional incentive for allies to attempt to match US

capabilities. What they failed to adequately account for was the important military benefit that can result from access to independent systems.

This benefit suggests that Nye and Owens's vision of an information umbrella must be updated. Rather than sharing data to maintain technological superiority, the United States should share its data to encourage partner contributions, interoperability, and resiliency. As Moltz identified, these attributes are the keys to twenty-first-century space power. The US should seek to be a coalition leader, just as Nye and Owens envisioned, but this coalition should aim to bring allies together to mutually share information in an "interoperable information umbrella."

Engaging with allies to encourage their technological development, rather than seeking to prevent it, is likely to generate stronger ties and reduce tensions. Acting as a leader in information exchange and interoperability also gives the US military greater flexibility in data-sharing decisions because allies are not entirely dependent on the United States. Thus, decisions to withhold some data have less of an adverse effect. Further, to the extent that data is shared, the United States can see concrete benefits as allies respond in kind, improving US military capabilities.

In the area of reconnaissance satellites, this stance could propel efforts to engage in more formal international coordination and data sharing with allies in Europe. The US would have multiple options for how to accomplish this. Rather than disclosing data from its most advanced, highly classified reconnaissance systems, it may opt to coordinate the development of jointly owned systems or to contribute data from a system specifically designed to complement allied capabilities.

For global navigation satellite systems (GNSS), cooperation and efforts to ensure interoperability with Europe's Galileo system are already well underway. However, it is worth noting that the US could have avoided much acrimony with its allies if this cooperative effort had begun a decade earlier. It may have a chance to do things differently by pursuing interoperability from the beginning if the United Kingdom moves forward with current plans to develop a GNSS.[43]

Data sharing and engagement are perhaps most advanced for SSA. The US Space Command, reestablished in July 2019, has continued the efforts begun by US Strategic Command to pursue data-sharing agreements that enable a greater degree of information sharing with partners.[44] These agreements also provide the United States access to data sources from many different entities and create an opportunity to understand and address challenges of system and data interoperability. Some nations—such as Japan, Australia, and Canada—have identified interoperability with US

systems as a goal for developing SSA systems.[45] The United States should encourage other nations to follow a similar path and engage with more independent systems, such as those being developed in the European Union, to explore options for interoperability early on.

As noted above, decision-makers have many options concerning how to assimilate the factors discussed here. There is no one-size-fits-all solution for all technologies, at all times, with all potential partners. Prestige, technical capability, economics, varied strategic interests, and other factors will continue to influence whether and when nations choose to develop independent capabilities. The dynamics of the security dilemma may play a role as well, and decisions to share data could help to alleviate or exacerbate the situation. However, this factor would likely be more relevant to sharing that extends to US adversaries rather than to allies.[46] In any situation, the United States must carefully consider the potential risks of sharing data or coordinating on technical development. However, the potential benefits of information sharing and the pursuit of interoperability should not be overlooked.

The examples above suggest that when US decision-makers determine how much data they are willing to share, when, and with whom, they should heed Nye and Owens's warning that these decisions may impact allies' decisions to develop their own capabilities. Nye and Owens argue that greater data sharing could be used to extend the period of US technical superiority. The examples described here suggest that the effect they identify is present, but their argument misses a key point. As noted by Moltz, with respect to information technology, redundancy and interoperability are often more valuable to national security than technical superiority because they can increase capabilities and provide resilience to the entire system. Data sharing is a way to gain leverage with allies and build coalitions, and when combined with engagement to develop interoperable systems, these relationships can be even stronger.

Conclusion

We have entered the information age, and as predicted by Nye and Owens, and argued by Moltz, our conception of power must adjust to this new environment. Nye and Owens argued that the United States should create an information umbrella, sharing data from its superior information technologies with allies to generate leverage and preserve technological superiority. They predicted that if the United States failed to share its knowledge, other nations would be incentivized to match its capabilities. This effect was seen in the cases of reconnaissance satellites, GNSSs, and SSA.

In the case of reconnaissance satellite data, the United States refused offers to provide imagery despite direct requests from close allies during conflict situations. With respect to GPS, the US provided non-US military users with a significantly degraded signal and emphasized its right to further degrade or disable the signal at any time. Changes to these policies proved to be too little, too late. Similarly, while the US proactively put in place a system for sharing space situational awareness data with foreign entities, it provided relatively low-quality data and gave no commitment to long-term provision. Even as systems for sharing space surveillance data have improved over time, the US has shown no interest in making its full high-accuracy catalog, raw sensor data, or algorithms available to its allies.

In each of these cases, US reticence to share data resulted in tensions with its allies and, ultimately, contributed to incentives to develop independent allied systems. However, these developments had critical benefits that Nye and Owens did not foresee in their assessment. The independent systems provide redundancy and resilience that underlie deterrence and, when systems are made interoperable, can result in appreciable capability improvements. As noted by Moltz, these disaggregated systems and cooperative relationships offer a superior model for facing twenty-first-century challenges.

To account for this advantage, the US should seek to lead the creation of an interoperable information umbrella. In spearheading this international cooperative effort, the US would share data with its allies. However, it would do so as part of a reciprocal system in which allies are encouraged to develop systems that can contribute data while also improving the system's resiliency as a whole. As noted above, the specific pathways to pursue this effort will differ depending on the timing, technology, and set of partners involved. This strategy recognizes the unique opportunity of the information age to maximize US power: strengthening relationships with allies, increasing system resiliency, and improving military capabilities. SSQ

Mariel Borowitz

Mariel Borowitz is an associate professor in the Sam Nunn School of International Affairs at Georgia Tech. Her research deals with international space policy issues, including international cooperation in satellite data-sharing policies and space security.

Notes

1. Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* 75, no. 2 (1996): 20, https://doi.org/10.2307/20047486.
2. Nye and Owens, 20.

3. James Clay Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," *Strategic Studies Quarterly* 13, no. 1 (Spring 2019): 66–94, https://www.airuniversity.af.edu/.

4. Robert L. Perry, *A History of Satellite Reconnaissance: The Perry Gambit & Hexagon Histories* (Chantilly, VA: Center for the Study of National Reconnaissance, 2012), https://www.nro.gov/.

5. Assistant Deputy Director for Plans and Policy, National Reconnaissance Office, to Col Von Ins, memorandum, subject: 156 Committee Recommendations, 12 November 1971, https://www.nro.gov/.

6. Bruce D. Berkowitz with Michael Suk, *The National Reconnaissance Office at 50 Years: A Brief History*, 2nd ed. (Chantilly, VA: Center for the Study of National Reconnaissance, 2018), https://www.nro.gov/.

7. E. L. Zorn, "Israel's Quest for Satellite Intelligence," *Space*, no. 1 (1991): 76.

8. Pierre Tran, "Space Intel Gives France Policy Independence," *Defense News*, 26 February 2015, https://www.defensenews.com/.

9. Peter B. de Selding, "Imagery Proliferation Has Diplomatic Cost for France, *Space News,* 8 July 2015, https://spacenews.com/.

10. Tran, "Space Intel."

11. Peter B. de Selding, "Germany's 2nd Military Radar Satellite Launched from Russia," *Space News*, 29 June 2004, https://spacenews.com/.

12. Peter B. de Selding, "French Helios 2B Spy Sat Sends Back First Test Images," *Space News,* 4 January 2010, https://spacenews.com/.

13. de Selding, "French Helios 2B"; and Jeff Foust, "IAI Sees Growing Demand for High-Resolution Imaging Smallsats," *Space News,* 6 September 2017, https://spacenews.com/.

14. US Department of Commerce, Bureau of Industry and Security, "Export Control Reform Spacecraft and Satellites," PowerPoint presentaton, 14 November 2014, http://bis.doc.gov/.

15. Dana Kim, "The 'Democratization of Space' and the Increasing Effects of Commercial Satellite Imagery on Foreign Policy," *New Perspectives in Foreign Policy* 18 (Summer 2019): 35–38, https://www.csis.org/.

16. Ulrike Bohlmann and Alexander Soucek, "From 'Shutter Control' to 'Big Data': Trends in the Legal Treatment of Earth Observation Data," in *Satellite-Based Earth Observation: Trends and Challenges for Economy and Society*, eds. Christian Brünner et al. (Springer International Publishing: Springer, 2018), 185–96, https://link.springer.com/book/10.1007/978-3-319-74805-4; Michael R. Hoversten, "US National Security and Government Regulation of Commercial Remote Sensing from Outer Space," *Air Force Law Review* 50 (2001): 253; Sarah Scoles, "How the Government Controls Sensitive Satellite Data," *Wired*, 8 February 2018, https://www.wired.com/; B. Schmidt-Tedd and M. Kroymann, "Current Status and Recent Developments in German Remote Sensing Law," *Journal of Space Law* 34, no. 1 (2018): 97; and Thomas Gillon," Regulating Remote Sensing Space Systems in Canada—New Legislation for a New Era," *Journal of Space Law* 34, no. 1 (2018): 19.

17. Norman Bonnor, "A Brief History of Global Navigation Satellite Systems," *Journal of Navigation* 65, no. 1 (January 2012): 1–14, https://doi.org/10.1017/S0373463311000506.

18. Peter B. de Selding, "Russia Pressing Ahead with Glonass Upgrades," *Space News,* 17 January 2012, https://spacenews.com/.

19. Bonnor, "Brief History."

20. Commission of the European Communities, *The European Community and Space: Challenges, Opportunities and New Actions*, Communication from the Commission to the Council and the European Parliament, COM (92) 360 final, Brussels, 23 September 1992, http://aei.pitt.edu/5806/.

21. Vincent Reillon, *Galileo: Overcoming Obstacles: History of EU Global Navigation Satellite Systems*, briefing (Brussels: European Parliamentary Research Service, April 2017), http://www.europarl.europa.eu/.

22. Office of Science and Technology Policy, National Security Council, "U.S. Global Positioning System Policy," fact sheet, 29 March 1996, https://clintonwhitehouse2.archives.gov/.

23. American Foreign Press, "US Warns EU about Galileo's Possible Military Conflicts," *Space Daily,* 18 December 2001, https://www.spacedaily.com/.

24. Barry James, "Washington Said to Fear Use of Galileo by Enemy in a War: U.S. Out of Line on Global Positioning, EU Says," *New York Times*, 19 December 2001, https://www.nytimes.com/.

25. Reillon, *Galileo*.

26. In October 2019, the US military began using the term "space domain awareness" to refer to this activity, emphasizing its view of space as a warfighting domain.

27. Rick W. Sturdevant, "From Satellite Tracking to Space Situational Awareness: The USAF and Space Surveillance, 1957–2007," *Air Power History* 55, no. 4 (Winter 2008): 4–23, http://www.jstor.org/.

28. *Commission to Assess United States National Security Space Management and Organization, Report of the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: Commission, 2001), http://www.europarl.europa.eu/.

29. Sturdevant, "From Satellite Tracking to Space Situational Awareness."

30. Tiffany Chow, *Space Situational Awareness Sharing Program: An SWF Issue Brief* (Washington, DC: Secure World Foundation, 22 September 2011), https://swfound.org/.

31. Mariel Borowitz, "Strategic Implications of the Proliferation of Space Situational Awareness Technology and Information: Lessons Learned from the Remote Sensing Sector," *Space Policy* 47 (2019): 18–27, https://doi.org/10.1016/j.spacepol.2018.05.002.

32. US Strategic Command Public Affairs, "USSTRATCOM, Polish Space Agency Sign Agreement to Share Space Services, Data," US Strategic Command News, 11 April 2019, https://www.stratcom.mil/.

33. US Air Force Space Command Public Affairs, "USSTRATCOM Expands SSA Data on Space-Track.org," 10 October 2018, Air Force Space Command News, https://www.afspc.af.mil/.

34. Bhavya Lal et al., *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)* (Washington, DC: Science & Technology Policy Institute, Institute for Defense Analysis, 2018), https://iislweb.org/.

35. Chow, *Space Situational Awareness*.

36. Lal et al., *Global Trends*.

37. Chow, *Space Situational Awareness*.

38. European Commission, *Report of the Panel of Experts on Space and Security* (Brussels: European Commission, 25 March 2005), 36, https://www.statewatch.org/.

39. Council of the European Union, "Council Resolution of 26 September 2008: Taking Forward the European Space Policy," *Official Journal of the European Union*, 26 September 2008, Publications Office of the EU, https://op.europa.eu/.

40. Regina Peldszus and Pascal Faucher, "European Space Surveillance and Tracking Support Framework," in *Handbook of Space Security: Policies, Applications and Programs*, ed. Kai-Uwe Schrogl (Berlin: Springer, 2020): 883–904, https://link.springer.com/.

41. Lal et al., *Global Trends*.

42. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), https://dod.defense.gov/.

43. Megan Gannon, "UK Ends Galileo Talks, Says It Will Explore a Homegrown Alternative," *Space News*, 4 December 2018, https://spacenews.com/.

44. US Space Command Public Affairs, "SPACECOM, Finnish Air Force Sign Memorandum of Understanding between Finland, US on Space Situational Awareness Cooperation," United States Space Command News, 4 November 2019, https://www.spacecom.mil/.

45. Lal et al., *Global Trends*.

46. Aleksander M. Lubojemski, "Satellites and the Security Dilemma," *Astropolitics* 17, no. 2 (2019): 127–40, https://doi.org/10.1080/14777622.2019.1641689; and Brad Townsend, "Strategic Choice and the Orbital Security Dilemma," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 64–90, https://www.airuniversity.af.edu/.

Russian Cyber Operations: Coding the Bounds of Conflict by Scott Jasper. Georgetown University Press, 2020, 214 pp.

The Stuxnet operation covertly affected Iranian nuclear ambitions while the NotPetya malware damaged Ukrainian systems and global infrastructure during the most well-known state-based cyberattacks. During the United States 2020 presidential election, the US had the same concerns as in 2016 of Russian internet troll farms attempting to manipulate public opinion. Confronting these arising problems requires understanding Russian cyber operations from strategic and technical perspectives. Fortunately, Dr. Scott Jasper examines these topics in *Russian Cyber Operations*, exposing the ways, means, and ends underlying Russia's various influence and attack events. Analyzing which Russian cyberspace actions breach armed conflict evaluations based on the *Tallinn Manual* and international norms, the model continues building on his previous work, *Strategic Cyber Deterrence*. The book explores Russian cyber practices through discussing recent active operations; ways where continuing operations affect international security dynamics; and, finally, US defensive options. The selected analytic framework allows Dr. Jasper to interweave Russia's strategic aspirations with tactical events. Each chapter highlights a case study demonstrating how the Russians applied the principle during recent operations. The work demonstrates exceptional documentation, careful research, and an appreciation for the subject matter's complexities. Those considering the strategic implications arising from state-based cyberattacks or any aspect of international tensions should add this volume to their reference list.

Dr. Jasper applies the strategic framework throughout the work based on groups possessing the technical means to conduct an attack and then whether attacks violate either legal standards or international norms. The technical aspect investigates the means used for intrusion, evasion, and deception and touches briefly on phishing and stolen credential attacks before reverting to a generic malware description as "malicious code intended to perform an unauthorized process" (p. 14). This oversight proves unimportant later as the work focuses more specifically on legal interpretation and US strategic approaches. The legal framework uses US Code, the UN Charter, and *Tallinn Manual 2.0* as written and published by the International Group of Experts to establish standards. The most used standards include violation of a state's sovereignty, intentional wrongful acts against a state, or the breach of existing international legal obligations. Technical and legal guidelines combine across the case studies to prove that Russian actors possessed the technical means and intended to commit wrongful, damaging acts.

Launching into well-documented events, the Cyber Operations section addresses asymmetry, hybrid attacks, and information warfare with separate chapters. Each involves a state use of cyberattacks against an unprepared enemy. The asymmetry chapter documents the 2007 Bronze Soldier event—where Russian patriots used distributed denial of service against Estonia to prevent removing a World War II memorial—before discussing the 2008 Georgian invasion. In evaluating hybrid warfare, a word for which no Russian doctrinal equivalent exists, Jasper substitutes the Gerasimov doctrine, an adaptive approach advocating military interventions at all societal levels. Hybrid warfare cases feature the 2014 Crimean and Ukrainian social media manipulation as well as the target tracking tool installed on Ukrainian military Android devices. Both events are analyzed as excessive intervention and unlawful use of force. The section's final chapter on information warfare assesses the 2016 Russian propaganda campaign and the Republican and Democratic campaign data breaches during US presidential elections. Though not violating the standard for an armed attack, the election interference events were still deemed unlawful as acts restricting the state's freedom of choice. Each section presents an interesting case while focusing more on whether an act breaches the legal standard than how those acts are technically achieved or integrated.

Continuing the strategic approach, the book's middle section reviews how state behavior creates reaction through discussing organizations like the Group of Seven and the UN Group of Governmental Experts (GGE) on Information Security. Jasper evaluates coordination between these groups as the primary method to establish norms and standards. The NotPetya case again demonstrates covert Russian actions as violating Ukrainian sovereignty, although the author questions whether damaging another state's private industry rises to a force-level event. Delving deeper into NotPetya's actions, Jasper suggests that neither Trump nor Obama's US diplomatic actions achieved the desired effect; legally indicting known Russian hackers and enforcing sanctions both failed to reduce Russian cyber campaigns. Finally, the text suggests that the *2018 Department of Defense Cyber Strategy* was designed to employ forward defense concepts to counter future Russian activity, even if many of those actions are not yet public.

The final section leans away from the analytic framework and case studies to suggest how future security strategies may offset projected Russian activity. The author first discusses how the National Institute for Standards in Technologies (NIST) Risk Management Framework (NIST 800-53) appears as one security standard for compliance options before mentioning Lockheed Martin's cyber kill chain. The cyber kill chain describes a rough format for how attackers penetrate and escalate privilege within a system. NIST cybersecurity practices appear frequently in US federal government compliance standards, but Jasper misses a step here through not using the same international standards applied during the book's first half. A standard chosen from either the European Union Agency for Cybersecurity (ENISA) or something associated with the UN GGE might have been more appropriate. The last two chapters continue those trends, demonstrating the Mitre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework; potential automated defenses; and how future technical offset might change cyber implementation. The technical offset chapter investigates a 2018 intercept of Ukrainian vessels by the Russian Navy, which was interesting yet unrelated to the overall cyber topic.

Dr. Jasper starts strong, with clear examples and excellent discussion about several past cyber events, notably the Bronze Soldier in Estonia and the Georgian invasion. After the strong start, I felt the book's latter sections moved away from the stated goal of exploring Russian cyber operations to focus on US strategic counters. After the two initial events, the only detailed attack reference was NotPetya and its Bad Rabbit predecessor. When selecting this work, I had expected detailed discussions about recent Russian cyberspace technical practices and strategic aspirations rather than a US policy debate. The book could have been immensely improved by taking a chapter or two to evaluate various players in Russian cyber or to compare known advanced persistent threats and their place as either government or military entities. Another missing feature was any comparison against multiple events either textually or graphically.

Overall, *Russian Cyber Operations: Coding the Boundaries of Conflict* effectively combines and categorizes several previous strategic theories under a common cover. The three sections allow the reader to review Russia's past actions, consider how states interact, and then move forward to US strategic options. Well referenced, with many current news and scholarly article links, the book demonstrates where future Russian cyber operations might affect US policy implementation. The text does fall short of the intended goal to comprehensively discuss Russian cyber operations, but my overall impression remains positive. I would recommend this book to those working federal government strategy or international relations and less to those pursuing cybersecurity fields. At the end of the

day, I did enjoy the work and will be adding *Russian Cyber Operations* to my own cyber policy reference list.

Dr. Mark T. Peters II, USAF, Retired

Warbot 1.0: AI Goes to War by Brian M. Michelson. War Planet Press, 2020, 421 pp.

Warbot 1.0: AI Goes to War is a science fiction novel of near-future conflict between the United States and China. In 2033, China has toppled the government of the Philippines. The US Army is on the ground to support the Filipino government and military in its efforts to retake Manila. This is the setting for a vivid, detailed tactical depiction of the impact of artificial intelligence (AI) and robotics on warfare.

In its focus on the transformational impact of tech, the book is in the same genre as the novel *Ghost Fleet*. Indeed, the author thanks *Ghost Fleet* coauthor August Cole for encouraging him to write the short story that eventually became the novel.

The author, retired US Army colonel Brian M. Michelson, served in assignments around the world in the XVIII Airborne Corps, the 101st Airborne Division (Air Assault), the 97th Civil Affairs Battalion (Airborne), United States Special Operations Command (USSOCOM), and Joint Special Operations Command (JSOC). As a senior fellow at the Atlantic Council, he focused on AI, robotics, and warfare.

There is no consensus definition of "artificial intelligence," which refers to software programs enabling machines to undertake tasks previously thought to require human intelligence. One of the principal approaches within AI is machine learning (ML). In ML, data is used to develop ("train") models that, given new data, can predict or classify rapidly. The models can be continuously updated with new data, with or without human supervision, allowing adaptation. These programs have a wide range of possible military applications, including navigation for autonomous vehicles, targeting, logistics, or the identification of unusual patterns of activity.

Warbot 1.0 is a novel used as a delivery mechanism for a payload of ideas about future war. AI-enabled robots fight alongside humans or in groups or swarms on land, in the air, and in the sea. The book opens with an engagement between US and Chinese autonomous armed vehicles. The Chinese rely on robots disguised as shipping containers to guard their installations and to identify and target Filipino citizens. Drone swarms seek and kill in urban combat, while groups of autonomous armed submarines target ships at sea and overflying planes. AI-driven robots identify, target, and attack at a speed that no human could match.

AI is also used to rapidly integrate and process multiple streams of information, from which it identifies patterns and makes predictions. Soldiers have improved, real-time situational awareness of the battlefield via receiving information and giving orders using virtual reality helmets and special gloves or exchanging with AI intelligence programs in natural language. Chinese psychological operations, directed against the families of deployed US soldiers, are individually tailored for maximum effect. Ultimately, the book concludes that US victory is delivered by means of human-AI teaming—compared to the Chinese reliance on AI alone—and a superior AI intelligence system that was easier to train and learn, enabling faster adaptation.

Warbot 1.0 also delves into some of the second-order effects of these technological advances. The use of robots in combat reduces human casualties, inviting military adventurism and allowing the use of tactics that involve sacrificing units without qualm. Conflict escalates rapidly when AI systems react to other AI systems. Real-time information streams tempt senior officers to micromanage, undermining mission command. Humans wrestle with ethically fraught decisions about settings that control the robots' level of autonomy and tolerance for civilian casualties. Humans anthropomorphize and develop

emotional attachment to the robots with which they work. Humans must decide how much they trust their AI systems.

The book's portrayal of the likely ways in which AI will transform war is broadly in line with current and emerging capabilities, even if the idea that all of these will be in place by 2033 is overly optimistic. Where the book is more fiction than science is in its portrayal of AI as working well and largely without error, even when predicting human behavior.

ML models are probabilistic, statistical models of phenomena developed from data sets. When the models are left to learn on their own, taking in data without human supervision, there is no guarantee of the outcome. If the data used to train the model is not representative of the phenomenon, the models may be biased or simply wrong. This is a recurring problem in facial recognition, for example, because most of the available images for training models are of men of European descent. Consequently, facial recognition is much less accurate for others. Also, if the underlying phenomenon changes in some important way, then previous data and models will no longer work well. This is why some stock market models were thrown for a loop by the COVID pandemic. Finally, humans can err in building models by failing to include important features; choosing the wrong algorithm; or making mistakes in data collection, structuring, cleaning, or coding. ML models work best when applied to concrete, clearly defined, stable phenomena for which there is representative data, and even then, they are sometimes wrong.

Warbot 1.0 does provide an example of an AI error due to novel input. It also acknowledges the probabilistic, statistical nature of machine learning models by imagining AI systems that communicate confidence levels for their claims and predictions, allowing humans to decide whether to trust that information. However, many of the things that would cause an ML model to be wrong—such as biased data, inclusion of the wrong features, or changes to the underlying phenomenon—would also make it impossible to calculate meaningful confidence levels. This, in turn, should have implications for human adoption of and trust in AI. The *Warbot 1.0* vision gives AI too much credit—but maybe that is what is needed for a good story.

M. A. Thomas
Air Force Cyber College

Satellite: Innovation in Orbit by Doug Millard. Reaktion Books, 2017, 208 pp.

What do you see when you look up at the stars? This is one of the fundamental questions that author Doug Millard, a deputy keeper of technologies and engineering at the Science Museum in London, tries to answer in his book *Satellite: Innovation in Orbit.* Millard dives into mankind's history and fascination with the universe beyond the planet that we inhabit and discusses the great minds and scientific achievements that made spaceflight and satellite launch possible. Written in a storylike fashion and densely illustrated, *Satellite* covers the full spectrum of launch into orbit and discusses the plethora of ways that satellites are integrated into daily life.

The book is organized logically, beginning with a discussion about the numerous physics discoveries contributing to the development and use of satellite systems. Sir Isaac Newton and Johannes Kepler are both introduced in the first chapter, which provides original illustrations from both scientists on their laws of gravitation and motion. Konstantin Tsiolkovsky's contributions make up a good portion of this initial content as well, and he is mentioned throughout the book for his work on applying the theories of earlier discoveries to rocket and propellant design. Particularly interesting are the parallels that Millard makes between prominent science fiction writers, such as Jules Verne and H. G. Wells, and the research that was making that science fiction a reality. This

connection to literary fiction helps to establish an early bond with the reader by referencing many familiar stories from these authors.

Millard quickly makes the transition from engineering theory to practice as the militaries of the world turn their attention toward acquiring and operationalizing these prototype systems being developed. Multiple think tanks and advisory groups, such as the RAND Corporation and the British Interplanetary Society, began devising solutions to the problems inherent in space travel. He covers the notable contributions of individuals, such as Arthur C. Clarke and several prominent Russian enthusiasts, to the concept of space lift. Millard also includes detailed images of the hobbyist groups and prototypes in action, engaging the reader in the excitement of the time period and giving a sense of belonging and wonder to this early space era.

Millard then expands upon the inevitable realization that satellites are being launched and used for all humanity. Rightfully beginning with a dialogue on Sputnik, Millard includes discussions on the early systems that were deployed for government use. He accurately summarizes the space race occurring between the Soviet Union and the US along with the public fascination as it all unfolded. The American launch of Project Score initiated the Western foray into the communications satellite realm, relaying a message from President Eisenhower across the globe for the first time. Millard furthers the discussion of early satellite uses, including expansion into reconnaissance with TIROS and imaging with SENTRY, as well as infrared detection using MIDAS. The intelligence agencies made quick use of these capabilities, employing them for data collection as the Cold War began to take shape.

As more powerful rockets are developed, Millard informs, higher orbits became more accessible (p. 106). This development created a market for global communications as commercial companies leveraged these rockets to place satellites in geostationary orbits. Telstar, *Intelsat-1*, and other satellites brought new methods of information distribution to industry and government. Details are also given about other orbits designed to solve unique challenges, such as the Molniya orbit, to cover higher latitudes. Satellite costs became affordable enough that large networks could be built, such as the Iridium constellation of 66 satellites. In this segment, the author introduces the Global Positioning System, which revolutionized precision navigation, timing, and nuclear detonation detection for military use. Millard wraps up the intriguing discussion of satellite constellations with a couple of chapters on their scientific applications. He spends this segment discussing the onboard elements, fuel types, propulsion systems, and orbits. Arming the reader with the history and functionality of satellites, he concludes by pondering the future of both satellite systems and mankind's presence in space. He leaves it to the reader to decide what the future holds.

In conclusion, Millard uses this book to introduce readers to the story of the satellite. His intent is simply to inform the reader of how humanity reached into its imagination to put objects into space and how that imagination can be put to use to usher in a new space age. It is an excellent book to place on the coffee table to entertain guests or to casually glance through at leisure. This book is not for those looking for a technical manual, but it will be appreciated by anyone looking to be entertained by and informed on the history and future applications of satellites.

Capt James Corcoran, USAF

The Button: The New Nuclear Arms Race and Presidential Power from Truman to Trump
by William J. Perry and Tom Z. Collina. BenBella Books, 2020, 219 pp.

The Button could have been a balanced, focused argument on nuclear deterrence and nuclear weapons. Ultimately, it devolves into the same tired antinuclear arguments of the

past 30 years. The work suffers from several limitations, first among them the conscious bias of the "usual suspects" cited in the work along with a plethora of hyperbolic statements. Some examples include the following: "We are all on the atomic Titanic. . . . The risk of accidental nuclear war is increasing. . . . [There is] very little in the way of controls. . . . We're playing Russian roulette with humanity. . . . There is no way to prevent a determined President from starting a nuclear war . . . without any provocation. . . . The system is unconstitutional, dangerous, outdated, and unnecessary." Additionally, the book is not logically organized to make the argument against nuclear weapons; rather, it presents the material haphazardly. It begins with a fantasy-based scenario likely to deter most serious nuclear scholars from reading any further. Next, the authors meander from current bluster, to some nuclear history, to a host of problems with nuclear weapons, then more history—but without a clearly focused argument or adequate context. The work would have been more effective by stating its arguments up front, then answering the question posed in chapter 9: "Why do we still have the Bomb?" Each problem or risk factor should have been addressed individually. Instead, the reader must wade through the disarray to reach the recommendations in chapter 10. This review begins there and analyzes each recommendation, offering a more balanced view of nuclear weapons and nuclear deterrence.

The authors' overarching argument is that the United States should ultimately eliminate all nuclear weapons, but until then, it should restrict authority for nuclear use and change its nuclear posture. They offer 10 recommendations to support this argument, summarized below.

End sole authority. The authors argue that presidents alone should not have the power to authorize nuclear use because they may be unstable or need to make a snap decision. Instead, Congress should be involved in any decision for first use of nuclear weapons to slow down the process and allow for more decision time. The president would retain sole authority to act freely and quickly in the case of a confirmed attack. The authors seem to believe that a president would, without provocation, make a nuclear-use decision without additional input. They conflate sole authority with sole decision-making, ignoring the consultations that would naturally occur before authorizing nuclear use—including whether use is legal in a given context. Such consultations were the case with President Trump's decision to deny a strike on Iran. While it may regrettably be part of deterrence, bluster is not blunder. Furthermore, requiring congressional approval could create ambiguity about who controls nuclear use and complicate extended deterrence. For example, if Congress voted to use nuclear weapons without presidential approval, based on the passions of the people, who decides? Does this ambiguity increase the risks that our adversaries might misunderstand US intentions or control? Such a situation creates a crisis within a crisis and may invite preemption by an adversary. The authors correctly state that control of nuclear weapons is scary. This is why the United States has sole authority.

No launch on warning (*LOW*). Perry and Collina are terrified of accidental nuclear use based on false warning, particularly from cyberattack or "if the STRATCOM Commander was having a bad day." They recommend using nuclear weapons only in retaliation after a confirmed detonation (on the US or allies). However, their argument discounts how LOW complicates Russian assessments of war outcomes and enhances deterrence. The work of Steve Cimbala is instructive here and could have been referenced to great effect.[1] The authors do not seem to realize that LOW is a US choice, not an automatic response. They fear LOW due to false alarms leading to an accidental nuclear war. The fact is, a nuclear accident is not war, and a nuclear war is no accident.

No first use (*NFU*). This recommendation may well be the most reasonable of the entire book. However, the argument for NFU is undeveloped and underexamined. On the one hand, NFU would appear to create a more stable deterrence environment because it offers a clear declaratory policy yet retains flexibility as a national security choice. How-

ever, such a policy is only as strong as the trust between adversaries—currently in short supply. On the other hand, NFU would not be reassuring to allies—especially if the authors' recommendation of congressional approval for nuclear use is adopted. This policy could lead to greater proliferation. The value of having options retains what Tom Schelling calls "the threat that leaves something to chance." Perry and Collina also suggest limiting the first-strike threat from submarines by restricting their deployment areas. This thinking is illogical. Since submarines are supposed to be stealthy, how would one know their location? And, even if restricted, their missiles could still be used for first strike.

Eliminate US ICBMs. This is the book's third major argument because it most closely relates to the authors' fears of false warning and LOW. They see ICBMs as simply a first-strike weapon of immense danger and not worth the yearly $10B replacement/sustainment cost over the next 30 years. While the authors support extending the New Start treaty limits on nuclear weapons, they fail to say what happens to Russian missiles not committed to US ICBM targets. They discount the "missile sponge" argument or using ICBMs as retaliatory weapons—even a sponge has holes. ICBMs impose costs on our adversaries and raise the stakes of an attack. Yes, the central US is in the crosshairs of Russian missiles, but without US ICBMs, what else would be in the crosshairs? Eliminating US ICBMs makes Russian targeting simpler and crucially more effective. These missiles are the safest leg of the triad and a worthy, affordable insurance policy for such an existential threat.

Renew New Start. While not a major argument in the book, the authors obviously want to stress the importance of arms control with a goal of nuclear zero. It seems the New Start treaty will be extended. However, the Russians do not intend to further reduce their strategic weapons or, seemingly, limit tactical/short-range nuclear weapons. The authors would like the US to immediately reduce its entire nuclear arsenal to 100 nuclear weapons and deploy only 10 nuclear submarines, without specifying a deployment posture or the effects on their other proposals. They somehow believe that such drastic reductions will make the US safer, ascribing much more trust to Russian intentions than to US military nuclear planners at STRATCOM. Finally, Perry and Collina predict grave implications from a lapse of New Start, claiming that a runaway arms race would be worse than current modernization efforts. This too is hyperbole. First, there is no current arms race, nor must there be one without New Start. Current modernization efforts respect New Start limits and will ensure that the systems remain viable. Nuclear weapons are not like fine wine: they do not get better with age. Second, as the authors mention, we do not need arms control to reduce our weapons—to even below New Start limits. How much is enough for minimum deterrence of a low-probability, high-consequence event? Is it zero or something else? This is a national security choice.

Limit BMD. The authors excoriate the US for deploying BMD, blaming it for most of our arms control problems and for Russian behavior. They posit that BMD is ineffective, costly, and destabilizing. Further, they fear that if a president believes missile defense is effective he may "escalate . . . [and] . . . the more we spend the more we convince ourselves it will work." This is fear mongering. By testing BMD, we learn what works and what does not. This process increases confidence in the system's ability to protect against a rogue state attack—buying time to consider retaliation. As for destabilizing, the US BMD system is not designed to defend against an attack from Russia or China. To think otherwise is ludicrous. Consider that the Russians have 100 missile defenses around Moscow. The US will soon have 64 systems in Alaska and California. The Russians would like the US to be completely vulnerable even though our systems will be extremely limited if used as a defense. Just as the US cannot assure allies, it cannot allay the suspicions of Russian leaders. Nations must convince themselves. Doing so requires trust and a trustworthy partner. The authors quote George Schultz's statement that "deterrence cannot

protect the world from nuclear blunder or nuclear terrorism." It seems reasonable to believe that BMD might.

The authors conclude the book with four more recommendations: using executive action rather than treaties to make unilateral changes to our nuclear posture, engaging North Korea and Iran, exercising public diplomacy toward nuclear zero, and electing an antinuclear president. Regrettably, few specifics emerge. However, earlier parts of the book suggest that they would prefer executive action to "de-mate" warheads from weapons to increase safety. They seek to increase public support for nuclear zero and, of course, the environmental and climate change benefits of nuclear abolition. Finally, they hope for a president committed to changing US nuclear policy. Success in the two latter efforts will require that the authors first convince Russian leaders of the need for change—something not likely until 2030 (post Putin).

The authors deal in possibilities without any analysis of probabilities and second-order effects of the risk of such drastic changes. They focus on US actions, neither addressing our adversary's actions and intentions nor suggesting turning Russian nuclear weapons into glowing ploughshares. The recommendations do not approach the kind of Reagan-Gorbachev moment of a grand bargain toward nuclear disarmament. Perhaps the authors were being realistic, but their fictional scenario makes it less likely. They could have suggested immediate, complete elimination of all ground-based nuclear weapons. Their argument remains unclear if the suggested limits (only 100 nuclear weapons) are unilateral or post–New Start goals for the US and Russia. However, since the book exhorts nuclear zero, suggesting anything short of zero seems useless. It would have been insightful for the authors to consider other more probable scenarios than the opening example. For instance, what should the US response be if we successfully intercept a rogue nuclear-armed missile launched against the United States? Even more interesting, what if the intercept fails?

Three recommendations are noteworthy: upgrade command-control systems, protect the president, and eliminate the Trident low-yield nuclear missile. C2 upgrades will make current and future systems less vulnerable and more effective. New methods of protecting the president will ensure continuity and proper authority. The authors should have suggested changes to presidential succession—to include the secretary of defense as third in line. Other options exist for a low-yield nuclear option that would help maintain submarine survivability.

The book proclaims that Bill Perry was the strategist behind most of the US military advantage today. If so, it seems strange his views have changed to such a degree. One wonders if this is part regret for unfinished work, missed opportunity, or perhaps an overzealous antinuclear coauthor. For those who believe that eliminating nuclear weapons is feasible, desirable, and acceptable, this book will likely disappoint. Those who believe otherwise will be equally unconvinced. A more balanced view of nuclear deterrence can be found in the writings of Forsyth, Chilton, Obering, Heinrichs, Mahnken, and Cimbala.[2] Read this book if you wish to learn the arguments of the antinuclear establishment, and remember that "it is well that *war is so terrible*, otherwise we should grow too fond of it."

Col W. Michael Guillot, USAF, Retired

1. See, for example, Stephen J. Cimbala, "Nuclear Arms Control: A Nuclear Posture Review Opportunity," *Strategic Studies Quarterly* 11, no. 3 (Fall 2017): 95–114, https://www.airuniversity.af.edu/.

2. See the *Strategic Studies Quarterly* archive at https://www.airuniversity.af.edu/.

Military Strategy: A General Theory of Power Control by J. C. Wylie. Rutgers University Press, 1967; Reprint, Naval Institute Press, 2014, 169 pp.

This reprint of US naval officer J.C. Wylie's *Military Strategy: A General Theory of Power Control* includes an engaging introduction written by John Hattendorf followed by the text of *Military Strategy* itself. The book also contains a postscript written in 1987 and three excerpts that offer additional insights into Wylie's theory.

John Hattendorf's introduction beautifully brings J. C. Wylie's career to life, shifting between his operational and intellectual experiences in the Navy. Wylie began serving in the Asiatic Fleet, where he had more experience with diplomacy than many of his counterparts who spent their interwar years engaged in fleet exercises (p. xi). Regardless, at Guadalcanal he showed himself to be a flexible and adaptable leader who innovated with new technology in combat to help his commander make the most of their ship's radar (p. xv). Subsequently giving him his first command of a destroyer converted into a minesweeper, the Navy removed him six months later to help it figure out how to help its officers systematically sort through the overwhelming amount of information that they had to process and comprehend (p. xvi).

Wylie's time at the Naval War College as a student in 1948 set him down the path of writing *Military Strategy* as—amidst the post–World War II throes of defense unification debates—the Navy struggled to justify its existence in an age of atomic weapons (p. xx). Seeking to make a powerful argument for what the Navy should do led him to the study of maritime history, particularly a broadened approach that examined the "relationship of maritime matters to events in other fields of human activity" (p. xxiv).

In doing so, Wylie accepted Julian Corbett's idea that the "purpose of sea power is to project control over the land" (p. xxvi). But Wylie wanted to do more than hone in on maritime strategy; he also sought to highlight the inadequate attention given to strategic thought in general (pp. 7–13). For example, although he considered US campaigns in WWII Europe to be "brilliantly fought," he concurrently assessed them as detrimentally having "an obscure, contradictory, and finally nonexistent strategic end" that sought peace more than control (p. 15).

Wylie believed that those who had studied strategy tended to either frame their analysis in discussions of offense or defense (pp. 17–18) or by identifying "principles of war" (pp. 18–19). His perception was that more attention needed to be devoted to "analysis by operational pattern" as well as "analysis on a conceptual or theoretical foundation" (pp. 20–21), which he broke down into four categories of maritime, continental, air, and Maoist (or revolutionary) war.

Wylie's analysis of operational patterns also led him to organize warfare by cumulative and sequential strategies. Wylie's sequential strategy consisted of a kind of linear progression of war through a "series of actions growing naturally out of, and dependent on, the one that preceded it," including the two drives across the Pacific in World War II (pp. 22–23). By contrast, submarine warfare in that conflict exemplified cumulative strategy, where the "entire pattern is made up of a collection of lessor actions" that are "not sequentially interdependent" (p. 23). Wylie believed this concept had as much applicability to air as to naval warfare (p. 25). He also thought that cumulative warfare could not be decisive in its own right; rather, its success "meant the difference between success or failure of the sequential" (p. 25). Thus, he wanted strategists to consider how to "balance our sequential and cumulative efforts toward the most effective and least costly attainment of our goals" (pp. 25–26).

Useful as these concepts were, however, he did not think that they were "adequate" for a holistic war theory (p. 27). Likewise, his conceptual theories of maritime, air, continental, and revolutionary or Maoist warfare also were not holistic, but he found them imperative for each service to better understand the others' way of thinking (p. 29) and to

determine "when and where and under what circumstances" each could be employed most effectively (p. 48).

Interestingly, Wylie believed that Mao's theory had been better tested than airpower theory (p. 53). Regarding airpower, moreover, theorists tended to assume that the "control of a people can in fact be exercised by imposition (or threat of imposition) of some kind of physical destruction . . . that . . . can be imposed from the air" (p. 63). Liddell Hart came closest to a general theory with his indirect approach, Wylie observed, but this concept was too "nebulous" and more or less just overlaid an indirect approach on top of continental theory (pp. 59–60).

Writing during the Vietnam War, he also wondered if and how a continental or Clausewitzian theory based on sequence could defeat a Maoist cumulative strategy or if the US must develop its own cumulative strategy (p. 54). Regardless, none of these largely domain-based theories offered a general and all-encompassing theory of war, not even Clausewitz (pp. 56–57).

Ultimately, Wylie wanted to determine "what kind of control is desired" in order to appreciate "under what circumstances will destruction or the threat of destruction bring about the desired means of control" (p. 41). Such control could be "direct, indirect, subtle, passive, partial or complete," and it also need not be military (p. 89). Thus, Wylie briefly advocated for crafting a compelling philosophy to "be 'for' " (p. 90), although he did not expand on this idea at length. But it fit into his insistence that—because "military matters are inextricably woven into the whole social power fabric"—a general strategy must account for "power in all its forms" (p. 93).

Despite being a naval officer, Wylie also believed that one of the key "basic assumptions for strategic planning" was that the "ultimate determinant in war is the man on the scene with the gun" (p. 72). To begin thinking about establishing control required one to determine the enemy's center of gravity or "national jugular vein" (p. 77), which then could be exploited by taking charge of the "pattern of war" by deftly "manipulat[ing] . . . the center of gravity of war."

A strategist must manage the "nature and the placement and the timing and the weight of the centers" toward one's desired ends (p. 78). General Sherman, for example, "manipulated the center of weight of the war as he marched" into the south, thereby seizing control of the war's pattern (p. 79). In World War I, the Allies attempted to act similarly at Gallipoli, although they failed (p. 80). On the flip side, one must also seek to make one's opponent's "theory invalid" in the planning process to keep the enemy from seizing control of a war's pattern (p. 86).

Wylie's *Military Strategy* offers a comprehensive and coherent look at military strategy that helps enable multi-domain operations by letting each service understand the other's worldview and then brings those perspectives together in seizing the initiative. Every *SSQ* reader should peruse this short tome on strategy.

Dr. Heather Venable
Associate Professor, Air Command and Staff College

Restoring Thucydides: Testing Familiar Lessons and Deriving New Ones by Andrew R. Novo and Jay M. Parker. Cambria Press, 2020, 198 pp.

"Wake any political scientist from a dead sleep with the words, '[T]he strong do what they can[,]' and they will likely finish the sentence, '[and] the weak suffer what they must' " (p. 119). This quote highlights just one of the many noted fortune cookie-esque sentences from which most individuals have derived their knowledge of Thucydides. Andrew R. Novo and Jay M. Parker, both professors at the National Defense University, find this knowledge problematic. As a result, they seek to bring their varied but reinforc-

ing backgrounds in history, classics, and international relations to bear on this relatively short, efficient introduction to Thucydides.

Their most repeated refrain centers on understanding the context in which Thucydides wrote to challenge the international relations' (IR) community's imposition of realism and structuralism onto his work. Thus, while they provide some overview of debates within the IR community about how to interpret Thucydides, most of their approach is historical in nature. They want readers to wrestle with the entirety of the text and seek to place it in historical context, and then they want readers to apply this approach habitually.

This book is especially timely in light of Graham Allison's oft-cited work *Destined for War: Can America and China Escape Thucydides's Trap?* The authors have not designed their work specifically to challenge Allison, but readers will certainly be prepared to do so upon completing this book. Their first chapter, entitled "Trap or Talisman?," provides context on Athens, Sparta, and other relevant Greek city-states as well as on Thucydides himself. The second chapter compellingly challenges systemic thinking that the IR community uses to portray a problematic bipolar world of Sparta and Athens. True to their historical thinking, the authors also resist the idea of an inevitable war between these powers. Rather, war broke out because of the choices made not only by Athens and Sparta—where citizens actively debated the use of force—but also by smaller allied powers. Major powers had to make tough decisions as to whether to provide support to uphold their alliances. In Sparta's case, this made the notion of Sparta hegemony a "chimera" (p. 46). That is not to say that Sparta was not powerful, but just that it had significant limits placed upon its actions by past decisions. Likewise, Syracuse and Corinth could be considered "major power[s] in their own right" (p. 53). This kind of context is essential to challenge the frequently quoted line about the inevitability of war between Athens and Sparta. Similarly, we should be careful to avoid making faulty parallels between Athens and Sparta then and the US and China today.

The next chapter unpacks the idea that fear pushed Sparta into war with Athens. The authors make a number of interesting observations about fear, such as pointing out the oddity of a city-state known so much for "courage and martial valor" acting out of fear in the first place (p. 90). A bit contradictorily, though, the authors then highlight that the most important Spartan fear may not have been of Athens but of their own helots (p. 91). This theme also reinforces the authors' continuing insistence that domestic realities and politics made essential contributions to decision-making in Athens and Sparta. They also identify a specific trigger for Spartan fear to keep readers from making simplistic, sweeping conclusions about how fear functions in international relations, noting that fear propelled Spartans into action when Athens "began to encroach upon Sparta's allies" (p. 92).

They reinforce the complexity of the Peloponnesian War by insisting on the "fragility of power and the fundamental flexibility of alliances" (p. 104), which dramatically emerges when one takes a wider view of the war than Thucydides. Furthermore, states struggle to measure power and, as a result, often make problematic and costly miscalculations (p. 173). This theme emerges strongly in subsequent chapters when the authors challenge the notion that the weak must endure what the strong can dish out. As the authors insist, the strong may do what they want, but they should also recognize the likelihood of painfully suffering from their own decisions (p. 120). This example is important when one considers the longer perspective of ancient Greek history—a perspective Thucydides failed to incorporate fully given his death before the ramifications of conflict had fully played out. For example, a strong Athens brutally destroyed the much weaker city-state of Melos even though Athens did not have to employ brutal force; rather, internal disagreements within the Melos government led some individuals to betray Melos to Athens (p. 133). But, even more importantly in the long term, no one really won in Greece. Athens fell in 404 BCE, yet the devastation continued, with Spartan

power later "shattered" in 362 BCE (p. 168). Ultimately, Athens, Sparta, and Thebes all "bid for dominance and failed" (p. 169). In other words, no one really won except later participants who benefited from Greece's disorder, reinforcing one of the authors' key points that the "winner is not necessarily better off than before the war began" (p. 174).

While this work never quite makes a case for how it differs entirely from previous works, it is an accessible treatment of Thucydides that provides invaluable perspective for students and professors alike, either before or after reading the ancient historian's work on the Peloponnesian War. Ultimately, the kind of issues the authors raise throughout help introduce students to complexity and the eschewal of simple answers to complex questions. This book will benefit students beginning a war theory course in professional military education or those more broadly enrolled in IR or history courses.

Dr. Heather Venable
Associate Professor, Air Command and Staff College

Mission Statement

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

Disclaimer

The views and opinions expressed or implied in *SSQ* are those of the authors and should not be construed as carrying the official sanction of the 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

We encourage you to e-mail your comments, suggestions, or address change to
StrategicStudiesQuarterly@au.af.edu

Article Submission

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

StrategicStudiesQuarterly@au.af.edu

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

View and Subscribe to *Strategic Studies Quarterly* at
https://www.airuniversity.af.edu/SSQ/

Free Electronic Subscription

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

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published by Air University Press, Maxwell AFB, AL.