Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Competitive Strategy Insights from Wargames

BENJAMIN JENSEN
JOHN T. WATTS
CHRISTIAN TROTTI
MARK J. MASSA

Scowcroft Center for Strategy and Security

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Forward Defense

Forward Defense helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces Forward-looking analyses of the trends, technologies, and concepts that will define the future of warfare, and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, Forward Defense develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition. This publication was produced in support of Army Futures Command as part of a project that used competitive strategy wargames to evaluate alternative long-term military investment strategies for great-power competition.

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Competitive Strategy Insights from Wargames

BENJAMIN JENSEN · JOHN T. WATTS · CHRISTIAN TROTTI · MARK J. MASSA

ISBN-13: 978-1-61977-121-5

Cover image: Army AH-64 Apache aircrews conduct formation practice at Camp Williams, Utah, June 5, 2019. In accordance with its Future Vertical Lift (FVL) modernization priority, the US Army plans to develop a new family of military helicopters that are better equipped for the future of warfare. *Source: US Army photo, US Army Flickr page https://www.flickr.com/photos/soldiersmediacenter/48050084687/in/photostream/*

September 2020

Table of Contents

EXECUTIVE SUMMARY

How the US military prioritizes future force-modernization investments has the potential to shape long-term geopolitical and military competition. Beyond increasing lethality, new capabilities also affect how rival great powers like China and Russia conduct strategic planning and make decisions on the types of forces best suited to challenge the United States.

To assess this dynamic, the Scowcroft Center for Strategy and Security and its *Forward* Defense practice area hosted a series of competitive strategy games to evaluate: how US national security professionals allocated resource investments across Army Futures Command (AFC) modernization priorities (Long-Range Precision Fires, Future Vertical Lift, etc.) in order to advance US strategy; and the extent to which these investments altered military strategy and defense-modernization programs in China and Russia, both played by subject-matter experts (SMEs).[1]

Two unexpected outcomes emerged. First, a new stability-instability paradox defined the competitive investment cycle.[2] Within the games, the United States focused on bolstering its conventional deterrent and warfighting capabilities through technology, but both China and Russia players responded to new US technology by funding proxy clients, the Belt and Road Initiative, cyber operations, and propaganda.[3] These players perceived that they could offset advanced US technology with indirect strategic approaches that distracted US policymakers and created suboptimal gray-zone environments, in which expensive and exquisite equipment would produce diminishing marginal returns (e.g., firing million-dollar missiles at irregular forces hiding amongst an urban population).[4] They also sought to bait the United States into launching protracted responses to complex, regional humanitarian emergencies and counterinsurgency missions, primarily as a means of undermining the United States' ability to make investments in disruptive military capabilities.[5]

The results produce counterintuitive findings for future force-modernization and force-design initiatives. Based on these insights, the United States should counter its competitors' asymmetric advantages by exploring low-cost ways to bolster US and allied forces operating in the contact layer and supporting gray-zone activities.[6] Potential remedies include additional investments in cyber, operations in the information environment (OIE), joint and allied interoperability, as well as intelligence and force multipliers for small adviser teams and special operators.

Second, new capabilities create new escalation risks. Russia players voiced concerns about inadvertent escalation.[7] They assumed that the extended ranges associated with modernized US long-range precision strike could be used against Moscow's strategic (i.e., nuclear) forces. Accordingly, they sought to attack these long-range fires early in a crisis or conflict, which could produce dangerous escalation spirals. There is a chance that the United States' Multi-Domain Operations (MDO) doctrine—which emphasizes Long-Range Precision Fires (LRPFs)—may trigger escalation pathways as new capabilities become operational, especially if confidence-building measures and clear signaling are not in place at the theater level.

1 On the Army's six modernization priorities and eight cross-functional teams, see *2019 Army Modernization Strategy: Investing in the Future*, US Army, accessed August 28, 2020, 6, *https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf*.

2 On the stability-instability paradox, see Glen H. Snyder, *The Balance of Power and the Balance of Terror* (San Francisco: Chandler, 1965) and Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca, NY: Cornell University Press, 1984).

3 Eli Berman, et al., "Introduction: Principals, Agents, and Indirect Foreign Policies" in *Proxy Wars: Suppressing Violence Through Local Agents*, Eli Berman and David A. Lake, eds., (Ithaca, NY: Cornell University Press, 2019); Gal Luft, *US Strategy Toward China's Belt and Road Initiative, Atlantic Council*, October 4, 2017, *https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/us-strategy-toward-china-s-belt-and-road-initiative/*; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018), *https://www.oxfordscholarship.com/view/10.1093/oso/9780190618094.001.0001/oso-9780190618094*; *Disinfo Portal, Atlantic Council*, 2018, *https://disinfoportal.org/*.

4 Benjamin M. Jensen, Henrik Breitenbauch, and Brandon Valeriano, eds., *Complex Terrain: Megacities and the Changing Character of Urban Operations* (Quantico, VA: Marine Corps University Press, 2019), *https://www.usmcu.edu/Portals/218/ComplexTerrain_web.pdf*.

5 Charles Cleveland, et al., *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Amherst, NY: Cambria, 2018), *https://www.cambriapress.com/cambriapress.cfm?template=4&bid=716*.

6 In discussions of Multi-Domain Operations, it is assessed that adversaries will use multiple layers of standoff in all domains (land, sea, air, space, and cyberspace—all the way to economic, information, and diplomatic) in order to dislocate and separate its various elements. Discussion of MDO is characterized by descriptions of different "layers" and the capabilities within them—e.g., the "sensing layer." The "contact layer" therefore, is a description of where much of the pre-war, non-lethal shaping activity occurs. It connects with the *Joint Concept for Integrated Campaigning* and joint concept of a new competition continuum.

7 Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, 4, Spring 2017, 50–92, *https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00274?journalCode=isec*; Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks*, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1992), *https://www.cornellpress.cornell.edu/book/9780801425639/inadvertent-escalation/*.

Other novel US military concepts and investment ideas, as well as key takeaways, included the following.

- **Capital-labor Substitution.** After the first round, multiple US teams sought to trade some operations and maintenance (O&M) and personnel costs for additional research-and-development expenditures (RDT&E). The teams viewed themselves to be in a critical, interwar-type moment wherein being left behind would produce significantly worse battlefield outcomes (e.g., a further transition from low-skilled/trained mass armies, to large semi-skilled ones, to smaller, highly trained/advanced-skill forces).

  Takeaways: Reassess legacy force-structure paradigms to identify what key characteristics and organizational constructs optimize the force to take advantage of new technologies like artificial intelligence (AI) and increasing autonomy.

- **Unmanned AI-enabled Networks Will Still Involve Expensive Human Capital.** US teams often used the first move to make initial investments in AI, on which they later capitalized during subsequent rounds. The investments tended to explore how to: increase operational tempo; counter propaganda; and detect new deception efforts associated with data poisoning.[8] Yet, some teams highlighted that they would have similar personnel costs in the future, but fewer people, as they accelerated programs to capture top talent and provide more immersive, realistic training.[9] Teams saw the benefit of smaller, highly trained forces able to take advantage of AI-enabled networks and large numbers of unmanned systems.

  Takeaways: Prepare the force for AI now. Ensure data can be ingested from training and operations, and ensure it is managed by highly trained personnel who understand when and how to adapt algorithmic inferences—i.e., they know when to trust and when to not trust the model.

- **Interoperable Joint and Combined Networks Can Be a Center of Gravity.** Multiple US teams sought to maximize investments that would allow them to better leverage the Joint Force and partner forces to create dilemmas for adversaries. This interoperability—whether built into future systems or purchased—was also a priority for cyber defenses and other measures designed to ensure resilience. Teams wanted to be able to connect to ensure they could rapidly aggregate and disaggregate relative to threats posed by China and Russia.

  Takeaways: Interoperability with the Joint Force will continue to be—and likely increase as—a force multiplier. This will not be generated from exercises alone. It requires hard discussions, imaginative thinking, and intentional investment.

- **Mosaic Warfare.** US teams sought to adopt the mosaic-warfare concept and build adaptive kill webs that could keep the enemy off balance. US platforms would be connected to each other via Future Vertical Lift and other assets, emulating certain US Air Force (USAF) concepts for F-35 employment.[10] These webs of small, distributed systems—many of which were unmanned—were seen as critical to providing survivable options for defeating aggressors in detail.

  Takeaways: This approach to war will not only require investment, but also conceptual and cultural shifts across all services. It is not optional; the US military needs to adapt or risk major defeat in the future.

- **Porcupines.** One US team sought to combat adversaries' asymmetric means by pursuing an asymmetric strategy of its own. Through low-cost capabilities like improvised explosive devices (IEDs), autonomous drones, and ground-launched missiles, this team potentially lowered the threshold for US intervention in defense of its allies and partners.[11]

  Takeaways: Sometimes creative assemblies of low-end capabilities create high-end effects.

8 For an overview of AI and military power, see Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, 3, May 2018, *https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/*; and Benjamin M. Jensen, Christopher Whyte, and Scott Cuomo, "Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence," *International Studies Review*, June 24, 2019, *https://academic.oup.com/isr/advance-article-abstract/doi/10.1093/isr/viz025/5522301*.

9 Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power, Center for a New American Security*, November 2019, *https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power*.

10 On mosaic, see Benjamin Jensen and John Paschkewitz, "Mosaic Warfare: Small and Scalable are Beautiful," *War on the Rocks*, December 23, 2019, *https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/*.

11 T.X. Hammes, *The Melians' Revenge: How Small, Frontline, European States Can Employ Emerging Technology to Defend Against Russia, Atlantic Council*, June 2019, *https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-melians-revenge-how-small-frontline-european-states-can-employ-emerging-technology-to-defend-against-russia/*.

Explore how to increase rapidly deployable lethality at lower echelons that denies competitors freedom of maneuver.

- **Enabler Strategies.** Multiple US teams sought to shift investments to focus on reducing the operating costs of fighting MDO at scale. These teams wanted to find low-cost ways of achieving efficiencies that allowed optimized intelligence, surveillance, and reconnaissance (ISR), targeting, and decision-making webs to simultaneously attack in multiple directions—a concept pioneered in earlier Army concepts like Force XXI.[12] The teams assessed that current capabilities were too expensive and required too much maintenance to generate sufficient tempo to attack in depth over time in a futuristic combined-arms fight. These teams thought that building magazine depth to signal the ability to conduct sustained combat operations over prolonged periods produced a deterrent signal.

  Takeaways: Invest in enablers that increase tempo, reduce operating costs, and free up resources to build magazine depth forward. These investments should prioritize intelligence synchronization and partner interoperability. Ensuring allies can create a common operating picture and shoot common munitions is a critical component of conventional deterrence and warfighting in the twenty-first century.

- **Commoditization of Technology Tends to Produce New Waves of Innovation.** As technology becomes cheaper, people experiment and find new uses for it (e.g., business cases such as networks, storage, and computers). The same probably goes for the military, which is likely on the verge of a new disruptive era that consolidates existing investments in third-offset technologies.[13] In this environment, what was once "differentiation" becomes "cost competition" (e.g., in mosaic warfare, the military would begin to focus on overwhelming through low-cost combinations).

  Takeaways: Revitalize tactical experimentation across the force. Shorten the distance between the lab and the battlefield by increasing force-on-force and wargaming experiments that assess emerging technologies and novel employment concepts.

12 On Force XXI, see Benjamin Jensen. *Forging the Sword: Doctrinal Change in the U.S. Army* (Palo Alto, CA: Stanford University Press, 2016).

13 On the third offset and its implication for landpower, see Paul Norwood and Benjamin Jensen, "How the U.S. Army Remains the Master of Landpower," *War on the Rocks*, October 1, 2015, *https://warontherocks.com/2015/10/how-the-u-s-army-remains-the-master-of-landpower/*; and Paul Norwood and Benjamin Jensen, "Three Offsets for American Landpower Dominance," *War on the Rocks*, November 23, 2015, *https://warontherocks.com/2015/11/three-offsets-for-american-landpower-dominance/*.

INTRODUCTION

Warfighting eclipses the moment of battle. Prior to the first blows, a defense strategy produces the concepts, capabilities, and formations that any operational or tactical leader finds at their disposal. Therefore, developing a modernization strategy for the US Army requires thinking more like General George Marshall and Major Albert Wedemeyer than General George Patton. In World War II, for instance, it was the Victory Program that mapped out how to scale combat power through the US industrial base, as well as investments in key capabilities such as the Higgins Boat, which enabled larger campaigns and key moments like the Normandy invasion.

The question is how to develop a military-modernization strategy in an uncertain era of multiparty strategic competition, in which private-sector technological breakthroughs seem to be eclipsing the "skunk works"-like, Cold War-era investment paradigm that presupposes secret government labs. In all likelihood, narrow AI (i.e., machine learning) and robotics have a different development trajectory than stealth. The breakthroughs in these areas will likely emerge in a commercial lab, not in an Area 51. This dynamic means that competitors could catch up before the United States leaps ahead.

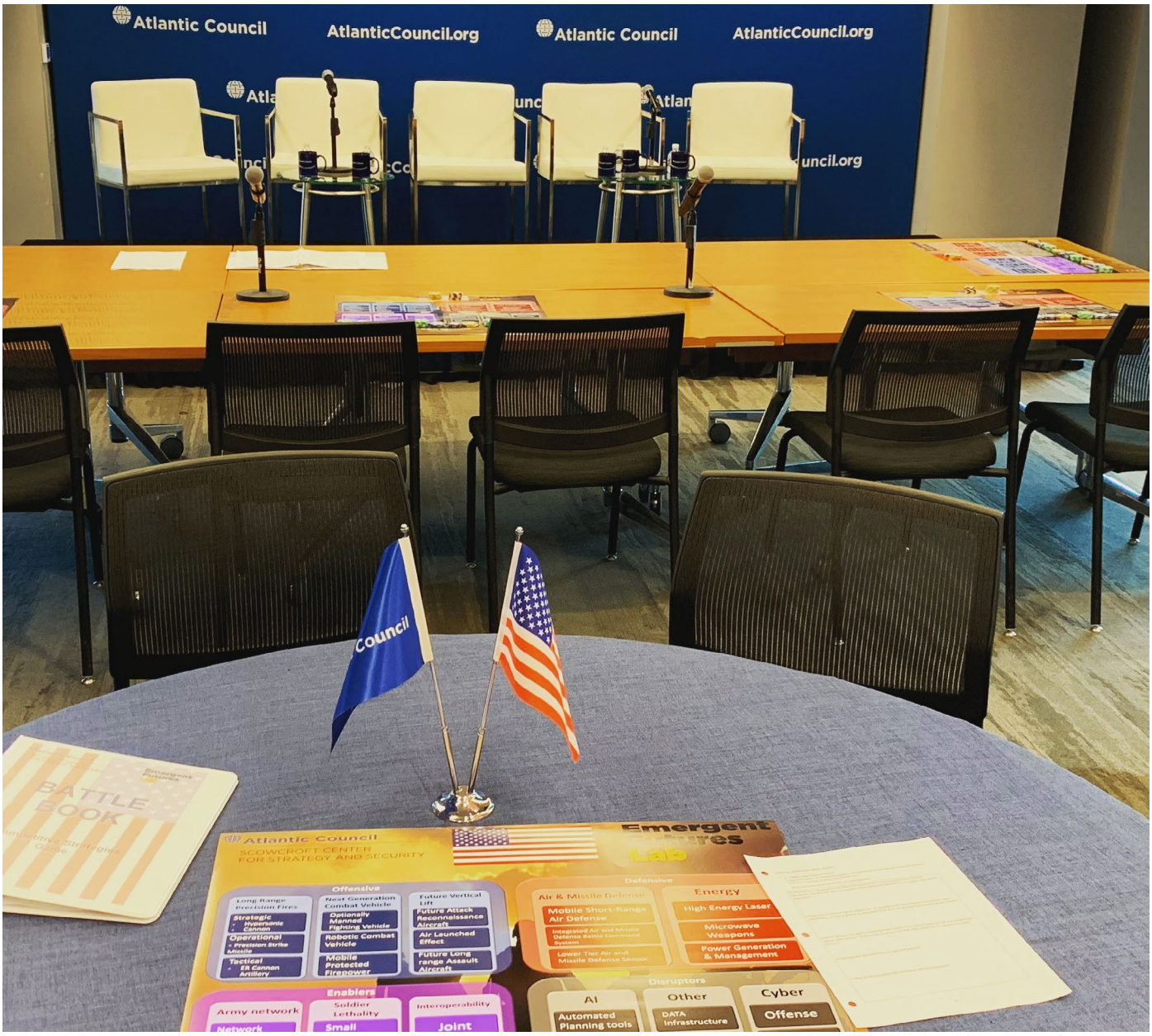
More than individual battles, defense strategy requires conceptualizing the actions taken to shape adversary decisions and position one's forces *before the battle starts*. It requires seeing oneself, the enemy, and the environment in terms of competitive strategies more than operational art. Wargaming this competition requires a new approach in order to replicate the diffuse, commercial-driven technology environment of today.

To that end, this project consisted of several competitive strategy wargames using a "matrix-game" approach that, instead of pitting a Blue Team combat formation against a Red Team combat formation, focused on modernization investments made prior to crises and battle. Each side made investments in a defense portfolio, balancing different requirements and making modernization bets in order to gain a position of advantage relative to its adversary. The teams contextualized these decisions within diplomatic, economic, and information actions that could amplify their military investments and consolidate long-term gains in competition.

APPROACH

This competitive strategy game consisted of teams representing the great-power competitors—the United States, Russia, and China—making investment decisions over five-year time horizons that reflect government investment timelines. Participants across all groups were composed of serving and former military officers, policy officials, and SMEs from the think-tank community. US teams acted in ways consistent with the *National Defense Strategy* and US service strategy to make investments using baseline, unclassified data on Research, Development, Training & Education (RDT&E) and procurement expenditures.

The game approach used a modified matrix-game dynamic. Starting in 2020, teams sought to develop and adjust



The first iteration of the wargame was conducted at the Atlantic Council. In accordance with their "matrix game" approach, the wargame facilitators developed physical tools to aid the players as they made decisions about modernization priorities, thereby creating a baseline for discussion. These tools included: gameboards unique to the US, China, and Russia teams; battle books providing further information on each capability set; and forms for self-reporting competitive investment strategies, theories of victory, and the process by which players linked means to ends. *Source: Atlantic Council photo*

Army Modernization Priority 1: Long-Range Precision Fires (LRPFs) to penetrate enemy anti-access/area denial (A2/AD) capabilities. This will likely include hypersonic weapons. In this photo, a common hypersonic glide body (C-HGB) launches from Pacific Missile Range Facility, Hawaii, on March 19, 2020, during a Department of Defense flight experiment. The US Navy and US Army jointly executed the launch of the C-HGB, which flew at hypersonic speed to a designated impact point. *Source: US Navy photo https://www.pacom.mil/Media/Photos/igphoto/2002267782/*

successive five-year modernization investments in response to the objectives and investments of the adversary teams. The Blue Teams (US) focused on developing an Army modernization plan while keeping other service priorities constant. The China and Russia Teams developed national modernization plans that accounted for the changes in the Blue Team's Army-specific plans. Adjudication of the moves was undertaken by a panel of experts with deep collective understanding of technology development, commercial innovation, military concepts, and operations, as well as noted futurists.

A game board mapped out modernization priorities for each team along with related technologies, while tokens representing million-dollar increments were used to represent the amount of RDT&E funding each team could anticipate having in that time period. Of note, teams were only allowed to adjust 10 percent of the expected RDT&E expenditure to replicate likely bureaucratic constraints to large-scale shifts in defense expenditures. In addition, teams had allocated funds in O&M, personnel, and procurement. They could move funds in or out of these areas to represent reprioritization of funding to align with their strategy, but could only adjust 10 percent in any one category to reflect bureaucratic constraints. A "basic research" area was also provided so teams could redirect available resources toward longer-term basic research focal areas in search of a long-term advantage.

Teams were tasked with developing a strategy for gaining a competitive advantage over their great-power rival(s). Once developed, they represented their plans on the game board and briefed their investment logic, including by

- defining their expected advantage (i.e., the theory of competition);
- explaining why they expected their declared investment(s) to achieve that competitive advantage; and
- articulating how the advantage supported their overall strategic objectives.

The following report summarizes the moves each team made during two iterations of the game.[14]

14 The first iteration was held at the Atlantic Council in Washington, DC, in July 2019. It was attended by a range of military officers, policy and strategy experts, technologists, economists, academics, and other SMEs. The second iteration was held later in July 2019 at the Marine Corps University School of Advanced Warfighting (SAW), and consisted of students enrolled in an advanced-planning course.

SUMMARY OF PROCEEDINGS: EVENT 1 Atlantic Council, Washington, DC

TURN 1 (2025–2030)

US Team 1

The first US team's theory of competition was a "porcupine strategy" focused on stopping Russia at the border of small allied states. It would entail small, hardened, and mobile strike sites that hold the enemy at risk, at range. This theory of competition would be operationalized by the transfer of inexpensive weapons to the Baltic States, prioritizing forward-deployed forces with the following three capabilities: improvised explosive devices (IEDs); cheap, fully autonomous drones; and concealable, long-range, ground-launched cruise missiles. On the game board, this meant investments in Long-Range Precision Fires (LRPFs) as a priority, as well as in integrated Air and Missile Defense (AMD), in the Army Network, and in machine-learning (ML)/image recognition to empower the autonomous strategic and operational fires provided by LRPFs. The intent was for small, mobile, long-range precision-strike units to tie down enemy forces and threaten their lodgments, thereby denying their ability to mass their forces and achieve a *fait accompli*, while simultaneously operating without complete communications. A potential consequence was that allies and partners may not be willing to shift from conventional military capabilities to asymmetric means like IEDs, thereby complicating the "porcupine strategy."

US Team 2

The second US team's theory of competition was enhanced network warfare—i.e., putting "the 'integrated' back in NATO's Integrated Air Defense System." Team 2 decided to integrate existing exquisite capabilities into the most efficient, secure, and resilient battle network possible. To achieve a resilient network, which could operate beyond the speed of human cognition, the team invested in network modernization, AI, cyber capabilities, and command and control (C2). They intended to create a future competitive environment in which the Army could disrupt enemy formations in depth. The key tradeoffs for this team were prioritizing the future at the expense of the present and prioritizing the integration of existing capabilities at the expense of procuring more hardware.

US Team 3

The third team's theory of competition was to maximize the Army's ability to compete in two distinct scenarios: conventional war and aggression short of war. In order to prevail in conventional war, this team invested in LRPFs and hypersonic weapons, which could be integrated with offensive cyber capabilities to suppress counter-battery fire. In order to defeat aggression short of war, Team 3 invested in assured position, navigation, and timing (A-PNT), thereby preventing deniable operations by irregular aggressors. Team 3 also bolstered joint interoperability in order to leverage the long-range firepower of other US services, while investing in network resilience, cyber defenses, and AI to defeat enemy attacks on the Army Network, both in peace and in war. Team 3 made a secondary investment in the Next-Generation Combat Vehicle (NGCV) to preserve the Army mission of holding ground. Its main assumption was that the US Army needs to compete both at a peer level and against asymmetrical threats. However, Team 3 was forced to cut the size of the Army, thereby redirecting resources into increased training and salaries to acquire talent in AI, ML, Internet of Things (IoT), and other advanced technologies. *More lethal* is better than simply *more*.

China Team

China's objective was achieving ascendency in the Western Pacific without provoking war with the United States. To achieve this objective, its strategy involved: deterring the United States from interfering with Chinese territory and interests by increasing potential US costs; building soft power through information operations; and investing in cognitive warfare. To operationalize the first component, China sought to expand existing anti-access/area denial (A2/AD) networks. These capabilities included better counterspace, conventional fires, and offensive cyber. The China Team debated the merits of hypersonics and concluded that a signal investment could force the United States to overspend. China made secondary investments in C2, as well as in the People's Liberation Army (PLA) Strategic Support Force to provide logistics enablement to these improved capabilities. In order to improve soft power and potentially cleave the United States from its Asian allies, China weaponized the Belt and Road Initiative (BRI) through minor additional investments designed to improve information campaigns.

Lastly, the team sought to build a substantive competitive advantage in cognitive warfare through AI and drone swarming, thereby pursuing a range of practical applications which could enable targeting and information distribution. AI could allow China to "leapfrog" the United States' technological overmatch. However, the China Team noted that its reliance on cyber and AI could prove escalatory due to the lack of existing global norms on the use of these technologies.

Russia Team

Russia's theory of competition was to escalate the competition within rival networks short of armed conflict, while maintaining the ability to race to preemption in the event of an apparently inevitable conflict. The Russia Team sought to operationalize network penetration and defense by investing in offensive and defensive cyber, C2, and electronic warfare (EW), while leveraging counterspace capabilities to limit US and allied sensor input into battle networks. Russia also pursued a long-range strike strategy, which would rely on LRPFs to: destroy forward-deployed US strike capabilities and disrupt the flow of US reinforcements, using unmanned underwater vehicles (UUVs) and unmanned aerial vehicles (UAVs) to target allied harbors and other facilities. The Russia Team feared a US cyberattack on its command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR) and industrial nodes, as well as a conventional strike against its nuclear arsenal, predicting uncontrollable escalation if either of these fears came to fruition.

Adjudicators' Comments

The adjudicators assessed that the players had maneuvered their way into a unique stability-instability paradox, producing different escalation dynamics. Network competition could lead to serious strategic first-strike incentives. The US Teams invested in automated systems and networks to determine who pulls the trigger first. Thus, increasing the speed of decision-making, especially through AI, could exacerbate volatility. However, the more that actors automate these tools, the more willing they may be to deploy automated systems against each other; accordingly, robot-on-robot warfare, in the absence of substantial human casualties, may reduce barriers to violence. Furthermore, within this new stability-instability paradox, the contemporary form of Cold War-era proxy wars may be subversive campaigns beneath the threshold of violence.

The adjudicators advised that the teams may need to reevaluate the political-strategic implications of their operational decisions. For example: US forward deployment could incentivize lethal responses; Russian and Chinese A2/AD systems may require more innovative US sustainment, which may alter regional basing and alliance constructs; and weaponizing AI would likely evoke political backlash. Additionally, the adjudicators were surprised that the US Teams did not directly invest in allied interoperability. If the United States is developing networks and AI to compete with its adversaries, it should include allies and partners. It needs to make investments in such a way that a US Army producing petabytes of data does not overwhelm an allied force that can barely process gigabytes. It is worth noting that during the plenary discussion, the China and Russia Teams stated that they were most concerned about some combination of the second and third US Teams' approaches.

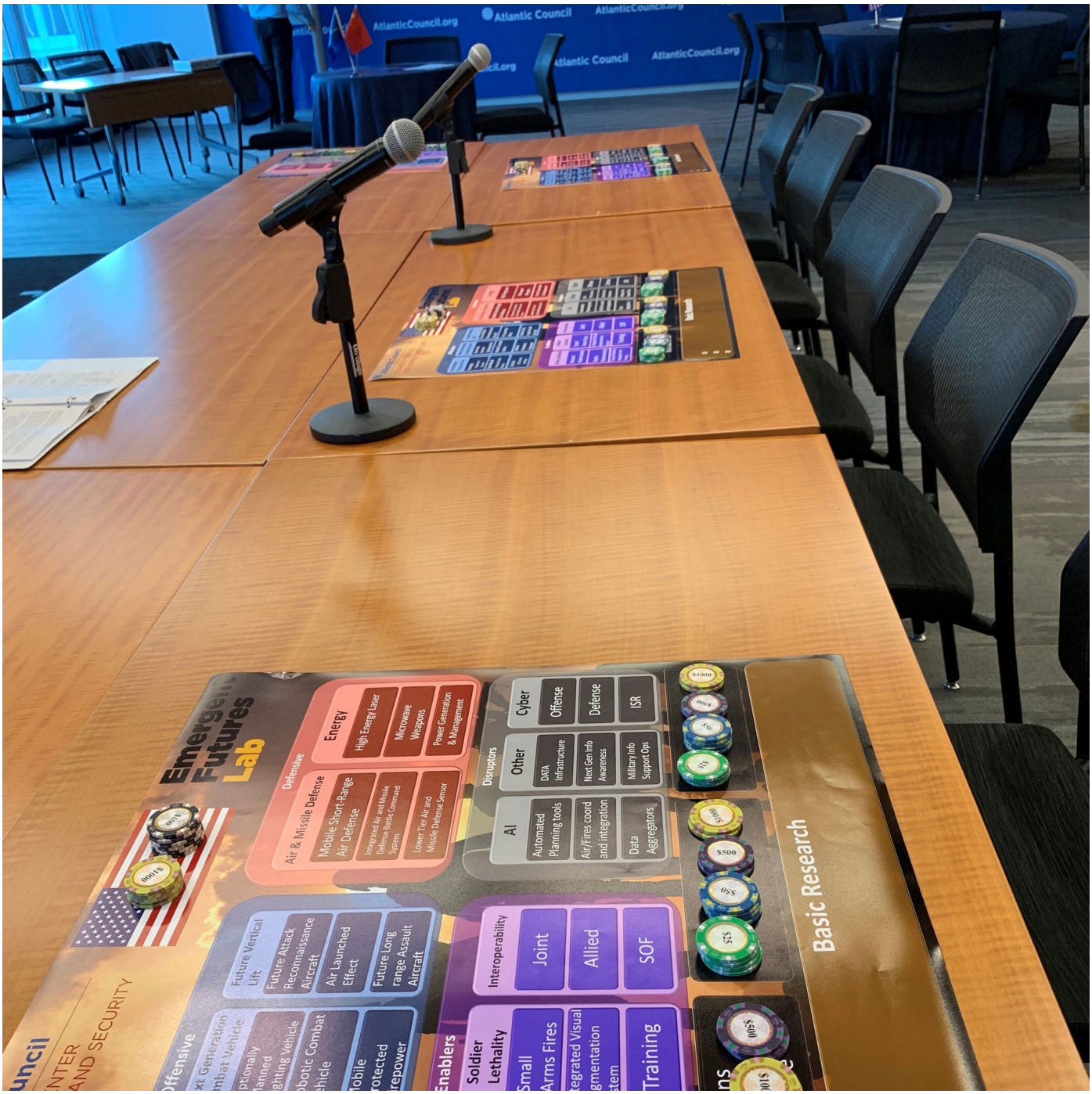
TURN 2 (2030–2035)

US Team 1

US Team 1 continued with "Porcupine Plus," while adapting to the adversaries' moves in the previous turn. US Team 1 considered adversary investments in air superiority and assault capabilities to be an attack on its porcupine strategy. Therefore, Team 1 aimed to shorten the "roll up" period of the porcupine strategy. The team invested heavily in training and Joint Special Operations Command (JSOC) interoperability to make the Army smaller and more elite. Because casualties amongst these relatively few soldiers could have a disproportionate impact on public opinion, Team 1 invested in Next-Gen Information Awareness to counter enemy propaganda. Investments in robotics were a further force multiplier. Team 1 also invested in cyber at the tactical level, allowing it to hack into video-enabled and contested environments. In addition to improving effectiveness, this modification was designed to assure allies by designing interoperability out of US systems, ensuring that the systems are automatically interoperable. Team 1 assumed that major US casualties could eliminate the domestic will to fight, especially if the losses were leveraged by adversary information operations. It also perceived any attacks on its network to be escalatory.

US Team 2

The second US Team maintained its network-warfare approach, while further investing in interoperability to capitalize on ongoing investments. For this team, interoperability meant investing in allies and partners, building sustainment and protection into the ground force, and bolstering infrastructure and standards within the host nations. To operationalize this strategy, Team 2 also moved 10 percent of the money in O&M to RDT&E in order to invest in enablers (e.g., AI/ML applications and networks, especially the new data infrastructure). The additional $2.5 billion reallocated from O&M was shifted into data infrastructure. This team



At the Atlantic Council, players used poker chips to indicate their military investments on the gameboard. The amount of money available to each team represented a consistent fraction of their respective country's defense budget. *Source: Atlantic Council photo*

assessed that personnel would be increasingly important as the Army relies on more sophisticated network technology; therefore, it invested in the people who will operate these tools. The team acknowledged that it probably should have undertaken this step during the first round. Its intent was for interoperability to protect and rapidly transition US and allied units forward in crisis. Team 2 assumed that the Army will continue to move away from a brigade-combat-team (BCT)-centric force to smaller, more lethal formations, which are better able to plug into the Joint Force and allied forces.

US Team 3

US Team 3 continued with its dual strategy of conventional standoff and network-centric competition, further cutting its size and concentrating training among the remaining troops. It sought to recruit top private-sector talent in advanced technologies. These highly skilled operators would facilitate the Army's interoperability with other services, allies, and special-operations forces (SOF). The team also intended to maximize integration of sensors and shooters facilitated by AI. While Team 3 also invested in ISR, Future Vertical Lift (FVL), and strategic deception, it claimed that these investments were part of the Army's planned modernization; its investments only added the additional network and AI capabilities to existing programs of record. Team 3 also assumed that data-sharing requirements with allies would be loosened, which would be necessary for maximization of its approach. Moreover, Team 3 predicted that its basic research investments in round 1, in ISR and signals, had matured and could be incorporated into the team's other investments.

China Team

China shifted its theory of competition from securing the Western Pacific to projecting its interests globally. The main method for doing so was the "intelligentization" of its forces and projection of power. China intelligentized the forces in which it invested during the first round by improving EW, C4ISR, and AI spoofing. China also focused on intelligentizing training by investing in hyper-realistic combat simulations and joint exercises between services and with partners, thereby accounting for its lack of recent combat experience. In addition to exercises, the PLA worked on officer exchanges and leadership training. China sought to become a major arms exporter, and the performance of Chinese equipment against US expeditionary interventions in the third world would serve as an information resource for improved Chinese influence. China would continue to gain fighting experience by deploying troops to UN peacekeeping missions, while selling an "authoritarian toolkit" that includes AI and 5G products.

Russia Team

Russia's theory of competition relied on igniting conflicts around the world while partnering with China to balance against the West. Russia continued to invest in LRPFs, cyber, C4ISR, and EW. The rationale for increased C4ISR investment was that a threat to command and control (especially that of nuclear and strategic systems) was fundamentally a threat to the state. Russia's cyber investment was meant to target the US commercial sector and elections, which are woefully unprotected.

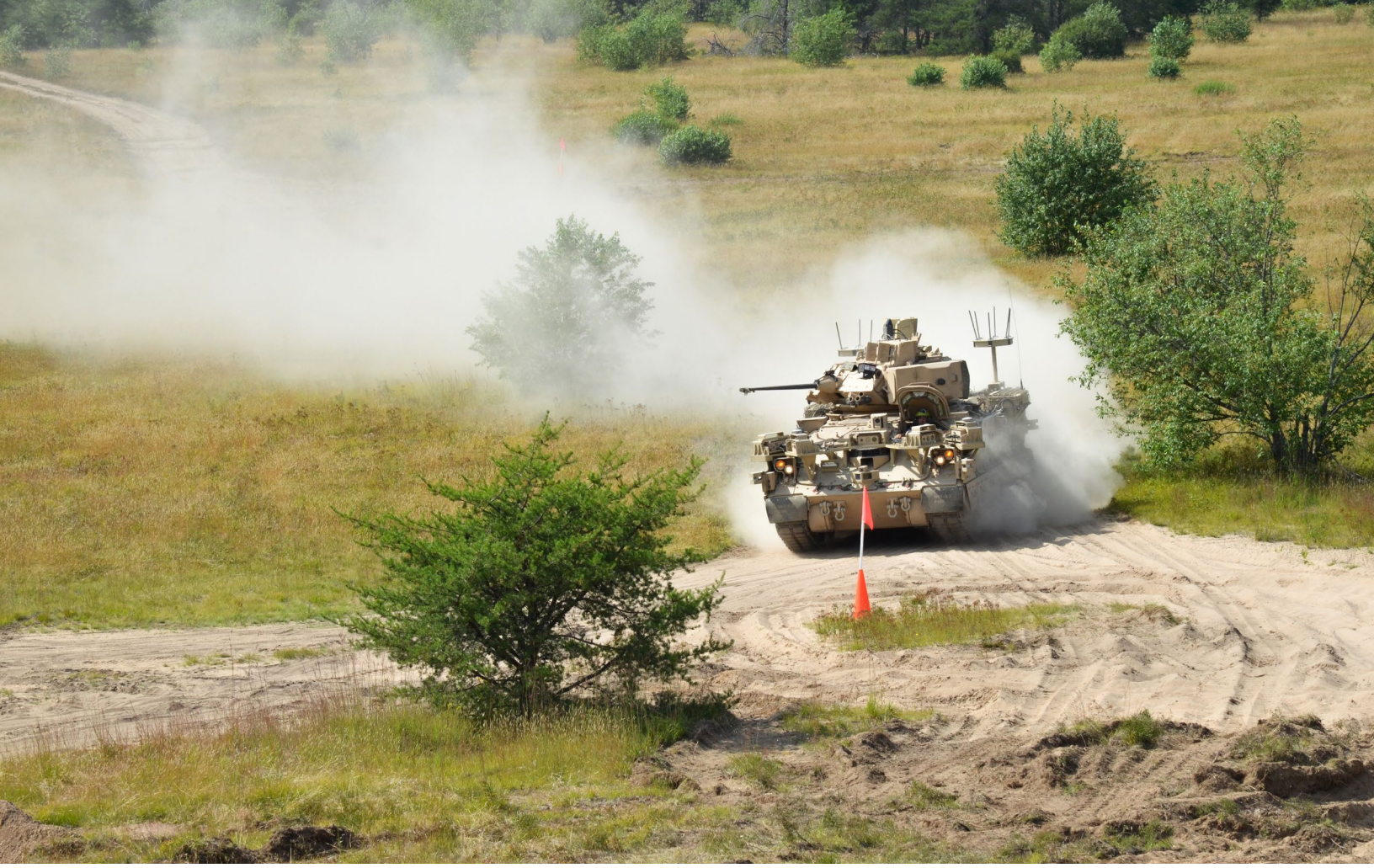
Russia assumed that it has been able to penetrate US networks. Moreover, it assumed that the United States had not sufficiently invested in offensive cyber capabilities to pose an existential threat. LRPFs are, however, very threatening to Russia. The Russia Team also assumed, after discussions with the China Team, that collaboration with China included exchanges of information on Western operating procedures in Ukraine and joint air patrols expanding beyond the northeast Asia region. This would expand to include joint submarine patrols in the Arctic Ocean. In addition, Russia bargained with China to receive the Office of Personnel Management (OPM) hack data to subvert US officials. Russia assumed that the reduced, elite force in which many of the US Teams were investing became a reality over the course of the game, and that the loss of one or two troop transport ships in the Atlantic would cripple US will in any European contingency.

Adjudicators' Comments

The adjudicators noted that the game featured the reemergence of small wars (within the stability-instability paradox) because large wars were not acceptable to any actor. As a result, Russia and China weaponized social media, BRI, and migrants, splitting the Europeans to cause the United States to increase its defense expenditures. Perfecting the art of killing becomes obsolete if each actor knows how to get the opponent to refrain from fighting in the first place—which explains why many of the teams focused, to some extent, on standoff across the spectrum of conflict.

The adjudicators were also interested in the emergence of capital-labor substitution. The teams created a new model for personnel, training a large number of people for specialized positions in order to better understand automated systems and sophisticated networks. This changed the labor model, so that the Army's labor could better use its capital to understand the patterns produced by adversaries, integrate data among services and allies, and better command and control in conflict.

The adjudicators also questioned the implications of non-state adversaries for military modernization. At what point should the United States shift from LRPFs to capabilities that can counter the clientalistic networks of its adversaries? Here, offsets are not necessarily technologically based, especially if the adversary is a parasitic elite class. It is not necessarily a military threat that adversaries fear the most—they can just turn to nationalism to rally their people against an external threat, so they often seek one out. Therefore, how does the United States hold the leaders of Russia and China at risk? It needs to discover what they are afraid of, and therefore consider dropping off next-generation virtual private networks (VPNs) to young activists, allowing citizens to take down their autocratic elites.



Army Modernization Priority 2: Next-Generation Combat Vehicles (NGCVs) to increase the firepower, speed, maneuverability, and survivability of land forces. Here, this Mission Enabling Technologies Demonstrator (MET-D) manned vehicle can operate two unmanned ground platforms to make contact with the enemy before soldiers do. *Source: US Army photo by Jerome Aliotta https://www.army.mil/article/226774/army_demos_prototype_manned_fighting_vehicle_teamed_with_robotic_combat_vehicle_platoon*

Game Conclusion

The players were struck by the fact that the US response was technological, rather than strategic. The Russia and China Teams were content with the result of this game, but the US Teams were content as well. This speaks to a limitation in the game structure, in that a more robust adjudication may have helped each team to better understand the inherent weaknesses in its plans and create tangible friction.

Another interesting idea was that interoperability could be an inhibitor due to its imposed costs. Therefore, it may be advantageous to build a different system of interoperability. Thus, even if an adversary strikes a network, the targeted system has redundancy.

The players noted that the China Team saw the United States as both target and teacher. Thus, the Chinese military appears to be becoming more American, which is what makes it a more formidable force in its operational concepts, strategic thinking, and focus on science and technology (S&T) rather than its personnel. However, this also creates certain weaknesses, for if the United States understands its own weaknesses, it could better target those of China.

SUMMARY OF PROCEEDINGS: EVENT 2
Marine Corps University

TURN 1 (2025–2030)

US Team 1

The first team's theory of competition, "Mosaic Airwolf," was designed to nullify Russian standoff through deterrence and compellence, using FVL and AMD. It invested in: future long-range assault aircraft and future attack-reconnaissance aircraft under FVL; mobile short-range air defense and an integrated air-and-missile-defense battle-command system under AMD; network modernization and A-PNT under Army Network; and in data infrastructure. This team sought to integrate other components by developing a network modernization necessitating joint (including SOF) and allied (i.e., NATO) interoperability. Investments were made to limit the likelihood of nuclear escalation.

This team assumed that Russian offensive conventional strike, defensive space systems, ISR enablers, and disruptive information operations would be the most robust threats to the Army's ability to conduct MDO. It also assumed that Chinese offensive maritime capabilities, defensive A2/AD, strategic lift and logistical support, and disruptive C4ISR would embody significant threats.

US Team 2

The second team's theory of competition was "Cyber Coalition in Conflict," aimed at denying Russian and Chinese actions short of war, especially non-attributional cyberattacks. The United States needed to modernize AI, cyber, and interoperability vis-à-vis NATO. The team also assumed that the Joint Force's primary challenge would be penetrating the adversary's forces, in accordance with one of the five missions outlined in MDO, but that the Army should not take the lead on this mission. Instead, it should integrate the Joint Force to ensure that the right capabilities are used. Therefore, the team relied on the Joint Force, investing one third of its resources into joint interoperability, and two thirds into cyber disruptors.

Through these investments, the team tried to transition to a future state in which the United States forward positions the Joint Force to enable penetration in accordance with MDO. This meant hardening the contact layer and repositioning SOF; improving the way the United States competes short of conflict through allies, forces, equipment, and doctrine; and achieving US data supremacy.

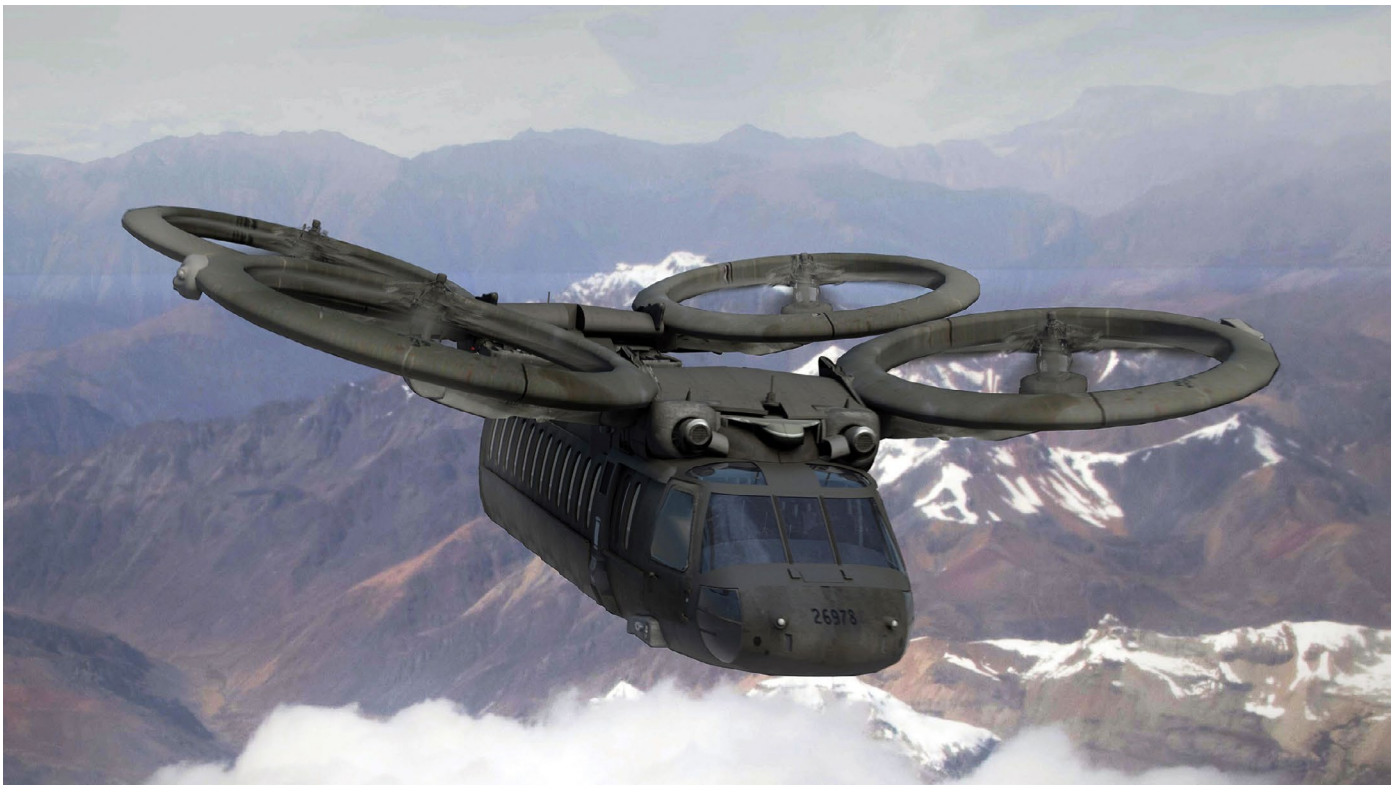
US Team 3

The third team's theory of competition, "Alliance Umbrella," aimed to maintain hegemony, establish freedom of navigation, bolster democracy, preclude a Russia-China alliance, and empower allies. The US Army pursued counter-conventional, counter-information, counter-gray-zone, and freedom-of-navigation capabilities. Accordingly, the team made substantial investments in ISR, AMD, interoperability, and AI to enable US leadership of a military alliance capable of defeating great-power rivals. This team pursued competition by cost in ISR, interoperability, SOF, and PNT, while pursuing both broad and niche competition by differentiation in AI.

The team assumed that the current state (i.e., the strategic environment) is one in which the United States is confronted by gray-zone threats and proxy wars. Therefore, its desired end state was one in which: allies defended themselves with US leadership; Russia and China were not substantively collaborating; global freedom of navigation was assured; there was continued US hegemony; Russia and China were internally stressed; and the decline in democracy was reversed. This team accepted several risks, such as the prospect of nuclear escalation and its own neglect in addressing adversarial LRPFs.

US Team 4

This team's theory of competition, "Digital Shield," was designed to counter Russia by improving allied interoperability, thereby signaling the United States' commitment to NATO and shrinking Russia's non-kinetic options. Accordingly, the team invested 20 percent into network modernization to mitigate Russian cyber disruption and 80 percent into allied interoperability. Team 4 assumed that Russia's investments in disruptors like cyber, information operations, and irregular forces—integrated into the new-generation warfare concept and focused on the first phases of conflict—substantially challenged the Army's ability to execute MDO. Specifically, disruptors enabled Russia to pursue strategic objectives while remaining below the threshold of war. The team predicted that US Cyber Command would lead in countering this threat, so the Army increased joint interoperability and cyber-force protection. The team acknowledged that by reducing Russia's non-kinetic maneuver space, its strategy would probably push Russia to more heavily invest in



Army Modernization Priority 3: Future Vertical Lift (FVL) to increase the maneuverability of Army aviation. The Joint Multi-Role Technology Demonstrator (JMR-TD) is demonstrating platform and mission systems technologies to help the Army make decisions about FVL capabilities, which could look like this hypothetical rendering. *Source: US Army graphic by Army Aviation and Missile research, Development and Engineering Center (AMRDEC) VizLab https://asc.army.mil/web/news-alt-jfm18-science-and-technology-supporting-future-army-aviation/*

disruptor countermeasures and in nuclear and non-nuclear strategic deterrent capabilities.

China Team

The China Team's theory of competition, "Attaining the Global Commons," assumed that the United States is a waning power and sought for China to be regionally dominant and globally balanced by 2050. The US military and its allies, in addition to China's own weak economic system and soft power, were the primary obstacles. The China Team sought to exclude the United States from the Second Island Chain, and therefore invested in: offensive nuclear submarines to offset US naval advantage, gain stealth, and project power; defensive A2/AD to offset the US naval advantage with low-cost solutions and deterrence by denial; enablers including AI, Strategic Lift, and logistical support to ensure information dominance, maritime basing, civil-military fusion, and power projection; and C4ISR and information disruptors to ensure information dominance and fracture US alliances. This team assumed that its strategy would produce significant risks, such as excessive focus on capabilities rather than personnel readiness, and on defense rather than offense.

Russia Team

With the approval of the game facilitators, the Russia Team presented a fake strategy during the first turn to potentially shape US counteractions, emulating Russian deception and disinformation. Its preliminary, deceptive theory of competition and investment strategy are as follow (the real ones are presented in the next section under Turn 2).

The Russia Team's deception (i.e., fake) theory of competition was to focus on deterrence above all else. It sought to maintain the status quo and to increase its global influence through access to global markets. The team primarily oriented its strategy to counter US investments in equipment and material that threatened Russian capabilities, especially capabilities that could undermine its nuclear triad. Accordingly, Russia invested 75 percent of its resources into strategic bombers, upgraded A2/AD to be distributed to allies, and ship-based ballistic missiles; 20 percent of its resources into disruptors and counterspace capabilities; and 5 percent of its resources into information operations to disrupt US domestic politics. It also dedicated basic research to space strike, autonomous Arctic underwater nuclear launch, and interoperability with China. It would operationalize this investment strategy through foreign weapons sales.

Army Modernization Priority 4: A modernized Army Network to improve command and control. Here, soldiers from 1st Stryker Brigade Combat Team, 1st Armored Division operate Stryker vehicles equipped with Warfighter Information Tactical Increment 2 (WIN-T Inc 2) networked systems as part of the Network Integration Evaluation (NIE) 15.1 test for record taking place through the end of October, 2014 at Fort Bliss, Texas. *Source: US Army photo, US Army Flickr page https://tinyurl.com/yyv4p4ey*

Adjudicator's Comments

The adjudicator assessed that all US Teams took interoperability more seriously than the think-tank teams had in the previous execution. However, they also undervalued the investment in people to train algorithms in ISR, in support of that interoperability.

The adjudicator also commented that US Teams 3 and 4 have turned alliances into redoubts against Russia, investing in a more survivable and resilient fixing force, which can hold Russia until the arrival of a mobile reserve. Thus, the alliance is the center of gravity, and hardening that alliance will impose costs on the adversary. This may be the right approach, but the adjudicator noted that it is possible they could be adopting the wrong perspective. Perhaps the Army should surge in a conflict, with the goal to secure communications, deliver fuel, signal resolve, and provide sustainment. Thus, an adversary could break the defensive line, but the United States would mitigate that threat with a more mobile Army capable of sustaining global power projection.

TURN 2 (2030–2035)

US Team 1

Overall, Team 1's strategy did not change. It increased investment in future attack-reconnaissance aircraft and future long-range assault aircraft as its primary focus, since the team believed that FVL possessed a competitive advantage in differentiation (especially through manned and unmanned teaming), which would allow the United States to circumvent armed conflict with Russia. Modernizing the Army Network was a main effort.

The team's supporting efforts were AMD (especially mobile short-range air defense (M-SHORAD)) to counter enemy LRPFs, joint and allied interoperability to mitigate the single-service (i.e., Army) focus of this exercise, power-generation and management to support FVL systems, AI air/fires coordination, and data infrastructure. It did not invest much in AI because it considered AI to be already incorporated in its existing investments (especially FVL). The team invested separately in AI for the fires and support mission, believing that US capabilities would reach a ceiling without AI.

The team assumed that Red Team investment in LRPFs would be most damaging to its strategy, but FVL sensor packages could connect with space-based systems that could help counter LRPFs.

The adjudicator assessed that this team's Army strategy allowed the other US services to counter and deter Russia strategically (e.g., through nuclear deterrence). Thus, this team preserved the Army's role in conventional deterrence as a surge force. This was not as escalatory a posture as those undertaken by the teams at the Atlantic Council execution.

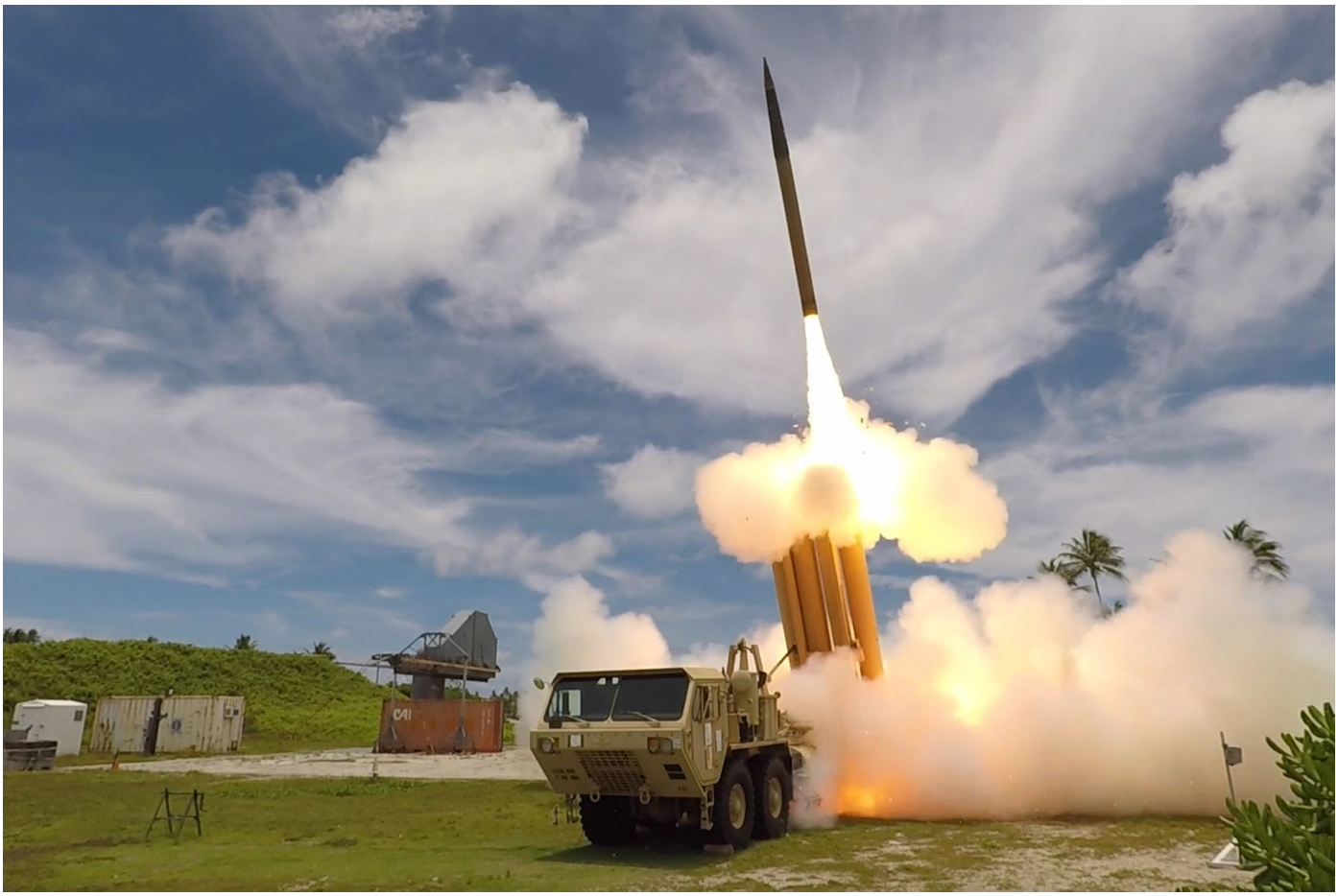
US Team 2

The second team modified its theory of competition, partnering with SOF units to compete below the threshold of armed conflict, supported by AI-enabled C4ISR. This strategy generated lethality from a smaller partner force, while the Joint Force penetrated and delivered follow-on forces. Team 2 renamed its theory of competition "Cyber Coalition in the Contact Layer."

Team 2 allocated Turn 2 resources to recruitment of skilled operators, emulating the approach of some of the teams in the previous execution at the Atlantic Council. This team assumed that the United States would be in a C4ISR race with its adversaries, and thus investing in the right people would be essential to victory. The team also wanted to compete in land forces, especially with SOF partners to US and allied conventional forces. This could create a significant surge capacity, as well as a present force that could compete below the level of armed conflict. However, this force could be perceived as escalatory, and it could lead to adversaries pursuing horizontal escalation to compete in the United States' "neighborhood."

US Team 3

In the second turn, Team 3 doubled down on power generation and management, which could increase mobility to



Army Modernization Priority 5: Modernized Air And Missile Defense (AMD) capabilities to defend US and allied forces and infrastructure from enemy aircraft and missile threats. In this photo, a Terminal High Altitude Area Defense (THAAD) interceptor missile launches during a flight test at the Ronald Reagan Ballistic Missile Defense Test Site in the Marshall Islands on August 30, 2019. Source: US Army Flickr page *https://tinyurl.com/y63c44ro*

be faster with fewer resources. Noting that the Navy and Air Force would have to counter Russian and Chinese investments in nuclear forces, Team 3 instead focused on adversary A2/AD, as well as AI and data enablers. Team 3 began to shift into offensive capabilities, focusing on strategic and operational LRPFs, as well as FVL as both an offensive and protecting force that could spoof enemy sensors to hide ground forces. The team did not return funding to personnel this turn, increasing training instead. Quality mattered more than quantity, as weapons systems became more sophisticated. The team also invested in all data categories, as well as in basic research on quantum computing to force adversaries to shift resources to that technological field. This latter move could be accompanied by an information-operations campaign to further concern adversaries and compel them to invest more in this field.

US Team 4

In accordance with "Digital Shield," this team invested in network infrastructure, training and doctrine development, personnel (especially expertise and retention), and procurement (including network/cyber modernization). Given adversary investment in strategic deterrence, this team decided to focus on network architecture and infrastructure, as well as interoperability with allies and partners. These capabilities required expertise and personnel. Money had to be allocated, of course, to procure the hardware for the original technology.

The adjudicator assessed that this team generated forces to move and fire in addition to dig in and defend. But, interoperability requires a defense-industrial base in allied and partner countries which could provide the logistical capacity for war (e.g., a common rail gauge, moving fuel, and facilities to reload vertical-launch cells on US surface combatants).

China Team

The China Team's ends and ways remained the same from the first turn, as it pursued "Attaining the Global Commons." It capitalized on its initial approach by investing in: defensive A2/AD, power generation, and resilience to bolster sea denial and impose costs on the US military; AI and data-incubator enablers to promote global investment and tap into human capital; and C4ISR disruption (i.e., cyberattack) and influence operations to deter the United States, ensure a second-strike cyber capability, and disrupt or degrade US relations with allies and partners.

The China Team's investments in AI incubators, within the United States and globally, allowed China to accrue competitive advantage over the United States by investing in US capacity. Investing in the US technological base, China could ensure that it works for Beijing. This would harm the United States as it tries to compete against an adversary that owns part of its industrial base. More threatening than Huawei's cheap 5G option, these checkbook political moves created "pink" adversaries, preventing the Department of Defense (DoD) from working with potentially compromised industry partners. On the other hand, this investment may create a vulnerability for China by exposing it to global financial markets, and thereby rendering it less threatening.

Unlike in the previous game, the China Team assumed that it needed to dedicate more resources to countering Russia, gradually decreasing its expenditures directed at the Untied States.

Russia Team

The Russia Team initially stated that there was no tremendous change from Turn 1. It kept the same percentages across the board. The team perceived that the primary risk was the threat to its nuclear triad, and did not see anything from the US teams that changed this approach.

The team then revealed its true strategy, which it had concealed during the first turn to emulate a Russian deception/disinformation campaign. The Russia Team perceived a disadvantage in physical forces, and therefore exploited misperceptions to create confusion and impose costs on the US teams. The Russia Team believed that it succeeded, as it saw Blue Team investment in expensive, aspirational, and possibly unattainable exquisite capabilities akin to the "Star Wars" program. Instead, Russia had actually invested heavily in disruptors, such as information operations, disinformation, weaponization of resources and trade, counter-drone warfare, and other cheap mechanisms. It also invested further in hypersonics and A2/AD.

For the Russia Team, victory meant that the United States focused more on China, Iran, and other threats. Russian foreign military sales to countries like Iran could produce that distraction, while also benefitting Russian oligarchs. In this way, Russia could become the *Arsenal of Autocracy*. One vulnerability to this approach, however, is that it would create disruption for the sake of disruption without an underpinning strategic vision. It therefore risks friction between Russia and China, as Russian arms sales to China could enhance China's ability to compete in Central Asia and elsewhere.

Army Modernization Priority 6: Increased Soldier Lethality, which involves improving individual soldiers' weapons, night vision, and access to data. Here, US Army paratroopers assigned to the 173rd Airborne Brigade conduct night operations while participating in Exercise Immediate Response at Pocek Training Area, Slovenia, on May 15, 2019. *Source: US Army Flickr page https://www.flickr.com/photos/soldiersmediacenter/47081187794/in/photostream/*

Game Conclusion

At the end of this second iteration of the wargame, the adjudicators were concerned about a mismatch. A force posture ideal for great-power competition may not be applicable in counterinsurgency, counterterrorism, or other limited contingency operations. Thus, a flexible mosaic program may be more valuable in responding to multiple potential threats. Small, cheap, networked systems that could plug into coalition sensors create multiple options for engaging targets ranging from squad-sized insurgent elements to adversary A2/AD nodes.

The participants and adjudicators also discussed an idea of thinking about the United States not as the *Arsenal of Democracy*, but as the *Incubator of Democracy*. Rather than simply supplying its weapons and capabilities to allies and partners abroad, it could work with allied countries on RDT&E, generating interoperable weapons systems with its partners.

It was assessed that strategic deterrence would hold, but the stability-instability paradox would be slightly different. Rather than proxy wars on the periphery, competition beneath the level of armed conflict may occur *within* the countries of NATO and major treaty allies like Japan, as hybrid challenges threaten domestic institutions.

Lastly, the teams discussed that Russia and China are far more afraid of protests within their own borders than of US military investments. The US Joint Force should consider this reality in calibrating its strategy and force posture to support broader competition objectives that leverage multiple instruments of power. In an age of increasing connectivity, global public opinion and domestic attitudes toward foreign policy could matter even to authoritarian regimes, and should therefore be harnessed in a manner similar to the early Cold War (e.g., Voice of America, Radio Free Europe/Radio Liberty).

CONCLUDING OBSERVATIONS

After running the competitive strategy game twice, resulting in seven different US concepts for defense modernization, a number of observations can be made.

- **Proxies buy time.** There was an interesting use of proxies and peripheral conflict to distract the United States while competitors caught up. A new stability-instability paradox produced a differentiation competition, thereby forcing the United States into markets in which it did not want to compete and spend the marginal defense dollar. In fact, proxy competition became a twenty-first-century form of global *petite guerre*.

- **The Blue Team enabler strategy.** Blue Teams focused on enablers that amplified existing Army cross-functional-team (CFT) investments. These enablers sought to lower the cost of achieving effects at scale through optimizing ISR, targeting, and decision-making.

- **Commoditization of technology tends to produce new waves of innovation.** As things get cheaper, people experiment and find new uses for them. For example, in business, the declining cost of networks, storage, and computer power were the catalysts for multiple innovations that power the information age. The same logic likely applies to the military and its initial investments in third-offset capabilities. Over time, what started as costly differentiation becomes cost competitive and unleashes operational and tactical innovation. This logic would imply embracing aspects of the mosaic concept and conducting multiple field experiments and wargames to let military personnel propose new use cases.

- **China will trade weapons for resources/access.** China is in a different strategic position than the United States or Russia. It has unique constraints, opportunities, and potential consequences for its actions. It will seek creative approaches to achieving its aims, facing different consequences than other competitors might face. Critical resources and access hold particular significance; thus, China is willing to use access to advanced weapons as trade incentives to achieve them.

- **Data poisoning as denial and deception.** As ubiquitous ISR assets proliferate, and it becomes easier to find, identify, and discriminate targets, adversaries will seek new ways to hide, camouflage, and deceive. Data poisoning is one, but not the only, new path to achieving these ends.

- **Magazine depth remains an issue.** Developing exquisite technologies (i.e., advanced capability) may create a temporary edge, but maintaining a sufficient quantity of them (i.e., capacity) to be decisive will remain a critical challenge.

- **The quantity-vs-quality equation may be changing.** The increased sophistication and complexity of weapons systems mean the armed forces may need smaller but higher-quality personnel (i.e., furthering the historical transition from "peasant armies," which now involves a transition from blue-collar to white-collar skills).

- **Key priorities may not be exciting.** Multiple US teams identified greater integration of the Joint Force and allies as key determinants of success, and highlighted the criticality of data infrastructure and security. Neither is an exciting capability, but both are massive force multipliers that could become critical vulnerabilities if neglected.

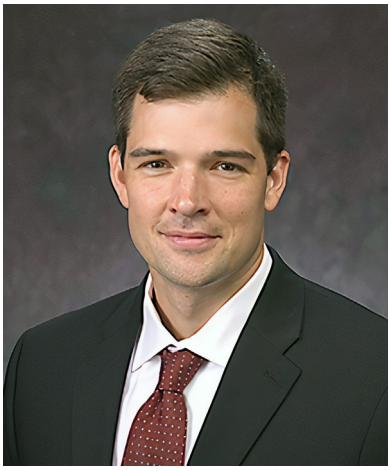
- **Perceptions of risk are difficult to predict.** In both games, the risks and threats posed by the adversary teams were very different from what was intended. This may be a result of the small representation of experts participating, or it may be indicative of the tendency to fail to understand the implications of strategies. Alternatively, it could mean that the creativity of some teams caught the Red Teams off guard. Regardless, deeper analysis of the impact of US strategies on a potential adversary is needed to better understand the relative value of the proposed future force-modernization initiatives.

Like all games—especially experimental ones—this approach had limitations. The budget numbers used were rough approximations for a number of reasons, and the game dynamics lacked direct friction between the adversaries. Because all concepts and investments were theoretical—and, in most cases, highly differentiated—it was difficult to apply rigor to the relative advantage of each approach. Nonetheless, it succeeded in developing a methodology and approach that was both engaging and challenging for participants, and valuable in developing new insights and perspectives on technology investment strategies for gaining a military advantage in long-term

competition. Additional executions would assist both in the iterative development of the approach, and to expand the community of interest thinking critically about the issues, while generating additional insights to add to the results summarized here.

In utilizing this approach, the game was able to explore a range of differentiated concepts for how future technology investment could shape future great-power competition. While no doubt limited by recency bias and current cognitive frameworks, the game identified a range of paths that could be taken in order for the US Army to gain a competitive advantage over its adversaries in the future.

About the Authors



In addition to being a senior fellow at the Atlantic Council, **Dr. Benjamin Jensen** holds a dual appointment as a professor of strategic studies at the School of Advanced Warfighting, Marine Corps University and as a scholar in residence at American University School of International Service. He recently served as the senior research director and lead writer for the US Cyberspace Solarium Commission.

Dr. Jensen has designed and participated in a wide variety of strategic and operational level wargames for the US Department of Defense over the last sixteen years including work with the Office of Net Assessment / Office of the Secretary of Defense (OSD / NA), Cost Assessment and Program Evaluation (CAPE), Defense Advanced Research Projects Agency (DARPA), Army Research Lab, Army Futures Command, the Joint Staff, Africa Command (AFRICOM), European Command (EUCOM), Central Command (CENTCOM), Indo-Pacific Command (INDOPACOM), and the US Marine Corps Warfighting Lab. Outside of the US military he has advised on futures-related studies, wargames, and scenario development for multiple major financial institutions including UBS, NATO, the US intelligence community, US Department of State, USAID, and the Economic Organization of West African States (ECOWAS).

He is the author of four books including *Military Strategy in the 21st Century: People, Connectivity and Competition* and a routine contributor to *War on the Rocks* and the *Washington Post*. In the past Dr. Jensen has received funding support from the Carnegie Corporation of New York, Charles Koch Foundation, Smith Richardson Foundation, Office of the Secretary of Defense Minerva Initiative, and Office of Naval Research. Outside of academia, he is an officer in the US Army Reserve.

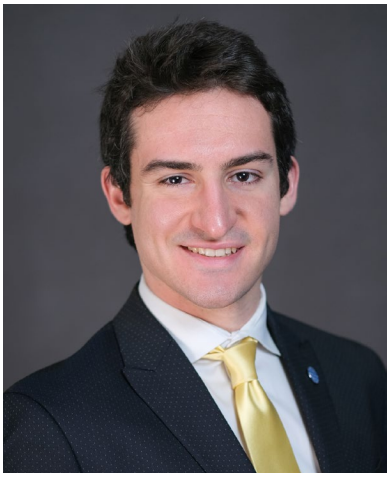
John T. Watts is a *Forward* Defense Senior Fellow at the Atlantic Council's Scowcroft Center for Strategy and Security, currently on secondment to the Office of the Secretary of Defense.

Watts has spent more than 15 years working across military, government, and industry, focused predominantly on the nature of future warfare and implications of complex emerging security risks. Watts has extensive experience leading high-profile wargames including on Middle East and Baltic security issues; countering terrorist and irregular groups; future concepts for the US Marine Corps and US Army; as well as the nature of game-changing technologies in warfare. He has also led research efforts on disinformation, 5G strategy, Indo-Pacific security, and alternate futures resulting from technology adoption.

He has previously been a partner at One Defense, a next-generation defense consulting firm assisting technology start-ups, and a senior consultant at Noetic, a boutique strategic consulting firm. Prior to moving to the United States, Watts was a staff officer at the Australian Department of Defence, working in a variety of strategic planning, implementation, evaluation, and management roles. Watts also spent more than a dozen years

in the Australian Army Reserves, where he held command, training, and officer development positions. He was also a liaison officer with the Virginia National Guard.

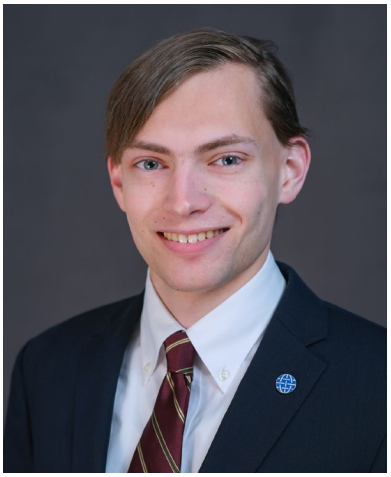
Watts holds a Masters in International Law from the Australian National University and a BA in International Studies from the University of Adelaide.



Christian Trotti is the assistant director of *Forward* Defense at the Atlantic Council's Scowcroft Center for Strategy and Security.

Having served as one of the Atlantic Council's lead action officers in building the new *Forward* Defense practice area, Trotti is responsible for executing multiple facets of program administration, including strategy, business development, and event and logistical planning. He has also authored and contributed to analyses on defense strategy, military technology, and nuclear deterrence, while assisting in the design and implementation of the Scowcroft Center's wargames.

Trotti is a *summa cum laude* and *Phi Beta Kappa* graduate of Georgetown University's School of Foreign Service, where he received his Bachelor of Science in Foreign Service with a major in International Politics/Security and a certificate in Diplomatic Studies. For his academic work, he was awarded the Joseph S. Lepgold Medal for outstanding achievement in the field of international security.



Mark J. Massa is a program assistant in *Forward* Defense within the Scowcroft Center for Strategy and Security at the Atlantic Council.

Massa contributes to *F*D research on nuclear security and arms control, the Future of DHS Project, the Commanders Series, and other endeavors. Having supported the launch of *Forward* Defense as the Scowcroft Center's newest practice area, he continues to carry out program administration in strategy, budgeting, business development, and event planning. He is a second-year master's student in the Security Studies Program at the Georgetown University School of Foreign Service. His research focuses on nuclear weapons, emerging technology, and the Arctic.

Massa graduated *magna cum laude* from Georgetown University with a degree in Science, Technology, and International Affairs. He was awarded honors in his major for a senior thesis on a theory of nuclear ballistic missile submarine strategy. He was elected to several honors societies, including *Phi Beta Kappa* (national), *Pi Sigma Alpha* (political science), and *Pi Delta Phi* (French).

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, *www.AtlanticCouncil.org*