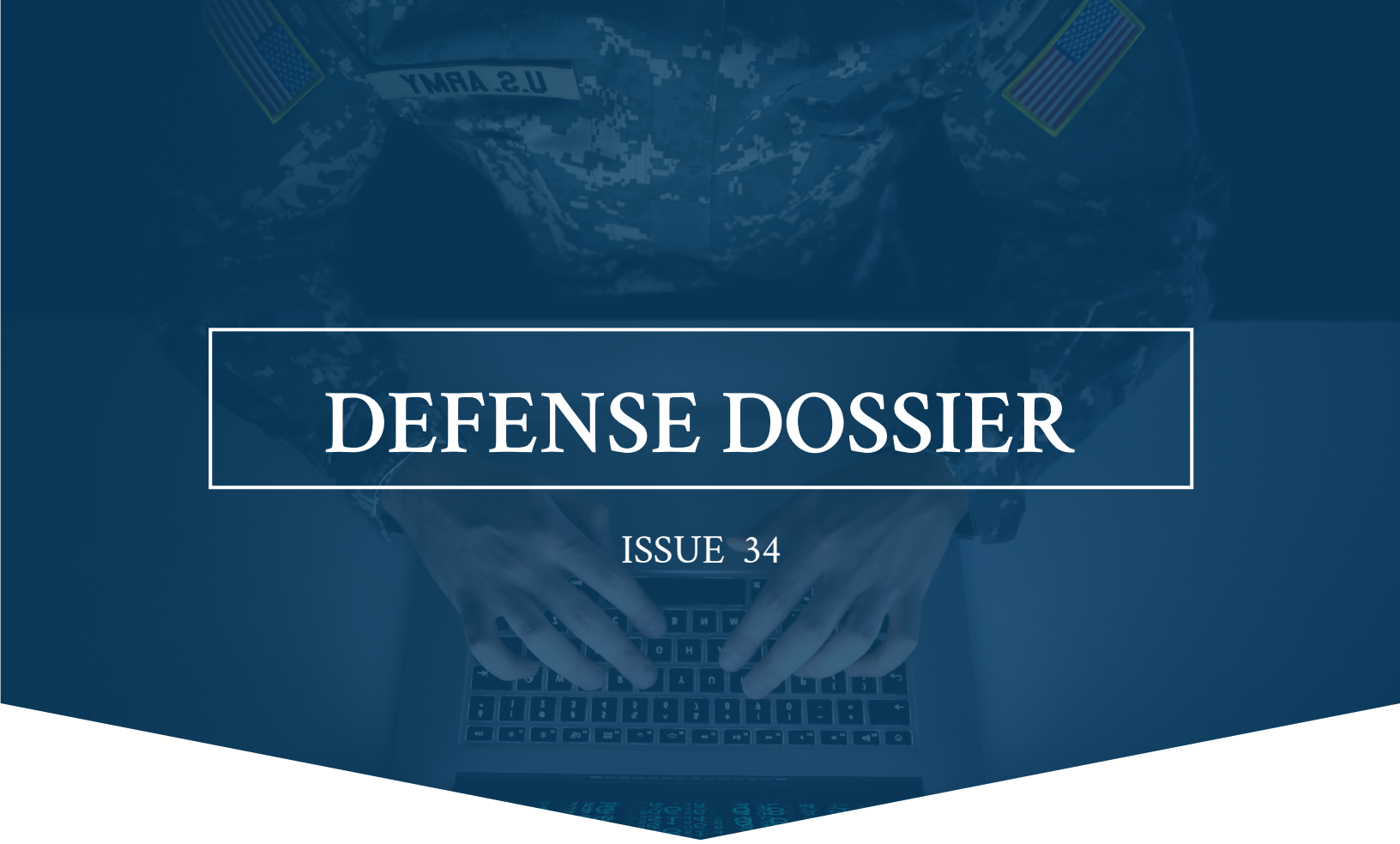

DEFENSE DOSSIER

ISSUE 34

OCTOBER
2022

AFPC

AMERICAN FOREIGN POLICY COUNCIL

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

DEFENSE DOSSIER

OCTOBER 2022 | ISSUE 34

LETTER FROM THE EDITORS

Welcome to the October 2022 edition of the Defense Dossier, the e-journal of the American Foreign Policy Council. In this edition, we assess the modern battlespace, and the evolution of technology that is both driving new threats to U.S. national security and responses to them. We explore how Russia's war in Ukraine has highlighted the effectiveness of asymmetric tactics, as well as the lessons learned to date from the conflict's non-kinetic battles. We examine the centrality of space to future conflicts, and the steps nations are taking to capture that high ground. We also take a look at biotechnology, a field that could potentially make an outsized impact on the evolution of the warfighter—and on national security writ large. And we assess the emerging field of wargaming, which is becoming essential to the modern warfighter. These challenges, and others, illustrate the dynamic, changing nature of today's battlefield—and provide important lessons for persevering in it.

Sincerely,

Ilan Berman
Chief Editor

Richard M. Harrison
Managing Editor

Assessing the Non-Kinetic Battlespace

Dustin Carmack

Kinetic warfare continues to evolve, though its brutality is enduring (as witnessed by the current war in Ukraine). But in the shadows, a preview of future conflict is playing out—that hybrid, non-kinetic future war.

Cyberwarfare, electronic warfare, information operations, intelligence, and space technology all came into play in the lead-up to the Ukraine war, and remain salient. The ongoing conflict offers many lessons that can help the United States and its allies not only to assist the Ukrainians in resisting Russian aggression, but also to prepare the West to prevail in future conflicts. All sides are keenly watching these "gray-zone" tactics play out, hoping to determine how best to use them for the battlespaces of tomorrow.

Prior to its invasion of Ukraine, the Kremlin had already used cyber and informational warfare, with varying levels of effect, in Estonia, Georgia, and Ukraine. Thus, when Russian tanks rolled into Ukraine in February, many experts expected to see coordinated, large-scale offensive cyber and electronic warfare operations aimed at severing communications in much of Ukraine. Also expected was a replay of previous power grid tactics meant to undermine confidence and stability in the government of Ukrainian president Volodymyr Zelensky.

The expected attacks did, in fact, come in the early days of the war. But many were stymied or blunted by cyber defense preparation, aggressive remediation, and timely assistance from allied partners and private-sector technology and cybersecurity companies who helped identify problems and provide solutions to Ukrainian networks. Microsoft, for example, identified and attributed a vast network of Russian activity that preceding physical battlespace movements in the war.[1]

Today, Russia continues to pursue aggressive hybrid actions in tandem with brutal land, air, and sea warfare. And allied and private sector partners continue to help Ukraine battle back. Through it all, these players as well as other world nations are watching to determine what has worked, and what has not. Those who learn the lessons now playing out in Ukraine will gain a greater understanding of how to deal with future shadow-war challenges—and, perhaps, how to use non-kinetic tools to deter or defuse kinetic conflicts.

THE EVOLUTION OF CYBER

When U.S. Cyber Command was officially stood up a little over a decade ago, strategists saw the need to invest in and understand our vulnerabilities in the internet domain, as well as those of our adversaries. Various strategies have been implemented since, albeit with fits and starts. Recently, significant attention has been devoted to boosting domestic cyber resilience, establishing a network of international partners, and increasing cooperation between the government and the private sector on matters of critical infrastructure protection.

For their part, adversaries and allies alike continue to test out various strategic roles of cyber. Historically, the "red line" for cyber operations has been ambiguous, unlike the *casus belli* for conventional warfare. This has caused new policy dilemmas which are as yet unresolved. In recent months, for instance, NATO has discussed that Russian cyber attacks on any Alliance partner could activate Article 5 collective defense provisions. [2] But what, exactly, is considered a substantive attack? Because of a lack of clarity on this front, it has led to ambiguous interpretations—and emboldened hostile actors to press forward with their offensive cyber operations despite the threat of a theoretical western non-kinetic or physical response. Hostile nations can likewise be expected to harness cyber against a range of vulnerabilities in the critical infrastructure, military

***Dustin Carmack** is a Research Fellow in Cybersecurity, Intelligence, and Emerging Technologies at The Heritage Foundation. He previously served as Chief of Staff to the Director of National Intelligence John Ratcliffe and as Chief of Staff to then-Congressman John Ratcliffe (TX-04) and then-Congressman Ron DeSantis (FL-06).*

establishments, and civil society mechanisms of western nations.

At the same time, multilateral cyber relationships in both the government and private sector are both growing and evolving. The United States has a critical role to play in this development. Because of its international standing, the U.S. needs to move beyond high-brow agreements to day-to-day engagements that can build trust and improve our overall cyber resilience and architecture.

The threat is very real. China, for example, is well known to be looking for a competitive advantage in the cyber battlespace, and its cyber espionage teams have consistently targeted the defense industrial bases of the U.S. and our allies in an attempt to understand, assess, and seek vulnerabilities.[3] This represents part of a larger—and disquieting—pattern; in time of both peace and war, skilled cyber adversaries will look to target and disrupt the data-rich network capabilities needed to properly provide command and control, intelligence, surveillance, and reconnaissance (ISR).

Just as space is getting more crowded every day with additional government and commercial actors, so too is cyber space. Since the invasion of Ukraine, a plethora of new actors has emerged. They include state and non-state sponsored entities, enigmatic "hacktivists," and criminal syndicates. All of these actors will continue to use cyber as a peace time tool for espionage, vulnerability exploration and exploitation, supply chain injections, and activities just below the threshold of armed conflict. Some, such as the Iranians, have continued to test the bounds of these vague thresholds in its proxy shadow wars with Israel and the United States. The addition of a swirl of hacktivists into the battlefields could likewise lead to missteps and accusations of state-backing or false flag operations meant to elicit a more aggressive response.

"Those who learn the lessons now playing out in Ukraine will gain a greater understanding of how to deal with future shadow-war challenges—and, perhaps, how to use non-kinetic tools to deter or defuse kinetic conflicts.

ELECTRONIC WARFARE, QUANTUM AND SPACE

Rapidly advancing technological developments in electronic warfare (EW) will be a major factor in any future conflict as well. The U.S., its allies, and its adversaries continue to pour resources into the development and environmental architectures needed to operate these systems amid a live fire conflict or as part of shadow campaigns.

As scholar Dean Cheng noted in the Heritage Foundation's 2022 *Index of U.S. Military Strength*, "Chinese military writings suggest that a great deal of attention has been focused on developing an integrated computer network and electronic warfare (INEW) capability…allow[ing] the PLA to reconnoiter a potential adversary's computer systems in peacetime, influence opponent decision-makers by threatening those same systems in times of crisis, and disrupt or destroy information networks and systems by cyber and electronic warfare means in the event of conflict."[4] The preponderant strategic goal of achieving "information dominance" sees Chinese electronic warfare capabilities as a complementary addition to the PRC's psychological and kinetic warfare.[5]

Last year, after a wargame "failed miserably," outgoing Vice Chairman of the Joint Chiefs of Staff Gen. John E. Hyten noted that, over the last 30 years, the U.S. had built its warfighting concepts on the assumption that it would enjoy unparalleled information dominance.[6] That assumption is no longer valid. China and Russia have invested heavily in building electronic, cyber, and space warfare capabilities to severely inhibit our military's ability to communicate fully and quickly. Building resilient systems, refining our own EW and counter-EW capabilities, and harnessing the electromagnetic spectrum in our favor will be crucial in any future conflict.

The U.S. Army Research Laboratory recently made significant headway in advancing the prospect of quantum electronic warfare. By using lasers to create Rydberg atoms, researchers were able to build a quantum sensor to detect the complete radio spectrum. This breakthrough could "unleash radical new potentials for

military communications, spectrum awareness, and quantum electronic warfare."[7]

For the military applications of quantum technology, the U.S. Defense Science Board has concluded that quantum sensing, quantum computers, and quantum communications are the most promising fields.[8] Quantum sensing will lead to significant improvements in submarine detection and prove useful in positioning and navigation. It could enable military personnel to detect underground structures, nuclear materials, electromagnetic emissions and enemy forces. Quantum computations will advance machine learning, which would enhance kinetic warfare systems by aiding the targeting algorithms of autonomous weapons—something that would revolutionize the battlespace.[9] The government could also make use of post-quantum encryption (PQE).[10] PQE remains a top priority for the National Security Agency (NSA), which is developing quantum key distribution and quantum key cryptography to protect military and U.S. government communications and information.[11] PQE would be resistant to both traditional and quantum-enabled decrypting software.

Future success in electronic warfare hinges on making technological advancements in artificial intelligence, achieving quantum superiority first, using quantum sensing and computation to develop advanced capabilities, and protecting our systems with post-quantum encryption.

INFORMATION AND COGNITIVE WARFARE IN THE AGE OF AI

Much has been written about informational warfare tactics of Russia and China in recent years. Recently, discussions have turned to the concept of "cognitive warfare," in which a nation state tries to alter public opinion and the resolve of leaders via technological developments in "AI, neuroscience, and digital applications like social media."[12] Col. Koichiro Takagi, a visiting fellow at the Hudson Institute, points out that, in terms of current technology, the PLA has considered the use of disinformation, preparation for operations of strategic nuclear weapons units, and various military exercises for intimidation purposes. Disinformation tactics could include "deception of enemy intelligence, surveillance, and reconnaissance activities by electromagnetic or cyber means to mislead the commander's judgment."[13]

In informational and cognitive warfare, it is essential to get independent, truthful information to those living behind autocratic lines. To this end, the U.S. must prioritize the development of technologies that can circumvent the censorship of our adversaries and preserve the privacy of those receiving the information.

Increasingly, the use of synthetic content in influence campaigns and technological advances in "deepfakes" for visual and voice are creating issues in today's fast moving digital environment. Even a subpar deepfake can circulate quickly. And, even if it is promptly identified as a fake, an initial presumption of legitimacy can produce the intended cognitive effect on an adversary.

In informational and cognitive warfare, it is essential to get independent, truthful information to those living behind autocratic lines. To this end, the U.S. must prioritize the development of technologies that can circumvent the censorship of our adversaries and preserve the privacy of those receiving the information.

Digital authoritarianism dynamics and technological advances around the world, especially from states such as China, will continue to challenge U.S. national security and American interests. Massive data mining collects vast stores of information that can jeopardize operational security and potentially produce cognitive effects on military personnel. Additionally, there have been rapid advancements in ubiquitous technical surveillance (UTS), facial recognition, and data collection from smartphones and vehicles. Advances in artificial intelligence will allow efficient sorting through these data inputs, producing valuable targeting information.[14] As such, understanding how China could exploit its surveillance and censorship technology—and how it might exploit its ability to collect sensitive, personal data on millions of Americans—is essential.

In response, the U.S. can lead the way by developing

technology, software, and algorithms to help repressed populations counter censorship and disinformation. This potential has been put on displace in recent weeks by Ukraine's use of SpaceX's Starlink satellite constellation to counter Russian information operations and allow Ukrainians freedom of communication in a denied environment.

NON-KINETIC WARFARE CAN'T WIN A FUTURE WAR… BUT CAN HELP DEFINE IT

If organized and conditioned properly, non-kinetic tactics (both current and future) can play a key role in any overall strategy. However, they cannot, by themselves, win a battle. As Gen. Patrick Sanders, Britain's chief of general staff, recently put it in the context of Ukraine: "You can't cyber your way across a river."[15]

Hard, kinetic tools still dominate an active battlespace, but hybrid activities can help shape battlefields. To persevere, those seeking strategic advantage in future warfare will need to integrate leading-edge technologies into their broader arsenals of conventional military tactics, systems, and strategy.

ENDNOTES

[1] Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," June 22, 2022, https://aka.ms/June-22SpecialReport.

[2] Jams Pearson and Jonathan Landay, "Cyberattack on NATO could trigger collective defence clause – official," *Reuters*, February 28, 2022, https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/.

[3] Lisa Ferdinando, "DOD Officials: Chinese Actions Threaten U.S. Technological, Industrial Base," *DOD News*, June 21, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1557188/dod-officials-chinese-actions-threaten-us-technological-industrial-base/.

[4] Dean Cheng, "Assessing Threats to U.S. Vital Interests: China," Heritage Foundation *2022 Index of U.S. Military Strength*, October 20, 2021, https://www.heritage.org/military-strength/assessing-threats-us-vital-interests/china.

[5] Ibid.

[6] Tara Copp, "'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight," *DefenseOne*, July 26, 2021, https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/.

[7] Tim McMillan, "Major Breakthrough in Quantum Electronic Warfare Achieved by Army Research," *The DeBrief*, February 12, 2021, https://thedebrief.org/major-breakthrough-in-quantum-electronic-warfare-achieved-by-army-research/.

[8] Kelley M. Sayler, "Defense Primer: Quantum Technology," Congressional Research Service, *Report for Congress*, Updated May 6, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11836.

[9] Katie Kline, Marco Salvo and Donyae Johnson, "How Artificial Intelligence and Quantum Computing are Evolving Cyber Warfare," The Institute of World Politics, March 27, 2019, https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/.

[10] National Institute of Standards and Technology (NIST), "Post Quantum Cryptography (PQC)," n.d., https://csrc.nist.gov/Projects/post-quantum-cryptography.

[11] National Security Agency, Central Security Service, "Post-Quantum Cybersecurity Resources," 2022, https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/.

[12] Koichiro Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," *War on the Rocks*, July 22, 2022, https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/.

[13] Ibid.

[14] Bill Gertz, "William Burns Backs CIA AI to Counter China," *The Washington Times*, February 24, 2021, https://www.washingtontimes.com/news/2021/feb/24/william-burns-backs-cia-ai-to-counter-china/.

[15] Daniel Michaels, "Lesson's of Russia's War in Ukraine: You Can't Hide and Weapons Stockpiles Are Essential," *Wall Street Journal*, July 4, 2022, https://www.wsj.com/articles/lessons-of-russias-war-in-ukraine-you-cant-hide-and-weapons-stockpiles-are-essential-11656927182.

Space as a Factor in Future Conflicts

Dee McHardy, Margaux Miller, and Peter Garretson

Space has been a key element of U.S. national security since even before mankind's first Lunar landing. Satellites, for instance, have been instrumental in modern military operations for decades, providing strategic intelligence on troop and equipment movements, detecting nuclear detonations and launches, and enabling unparalleled military readiness through missile warning, precision timing, and overhead reconnaissance. Simply put, space technology has made America the dominant military power that it is today.

But as space technology continues to advance, can the U.S. maintain this strategic advantage? What new advancements in space operations have the potential to give us an edge over our contemporary competitors? And which of them present a threat to our security and primacy? The answers to those questions will help shape American attitudes toward space – as well as the place that space occupies in our national security calculations.

GRAY ZONE WARFARE

Satellites have been a key component of American military and commercial might for the last forty years. And today, thanks to advancements in technology, satellites are far more common in both the private sector and the militaries of other spacefaring nations. In turn, this new field of near-Earth space technology has opened a new and complicated area of conflict.

First, the gray area between neutrality and direct involvement in a conflict has widened even farther. Once upon a time, the U.S. could send weapons or advisors to aid a nation in a conflict zone without directly dispatching troops. Now, the U.S. can offer significant advantages to allies in combat without sending a single officer or weapon—simply by providing space-gathered intelligence. By sharing geospatial intelligence, for instance, the U.S. has been aiding Ukraine in defending itself against Russia's current onslaught.[1] This aid comes at both minimal risk and cost to the American public, but provides significant advantages to the Ukrainian military. This expanded gray zone in military conflict is undoubtedly a boon to U.S. interests in the present conflict. However, it also provides the potential for adversarial spacefaring nations to do the same in future scenarios.

Another unforeseen outcome of space technology becoming widely available has also played out in Ukraine: private citizens can now take active, impactful roles in conflict. When Russian artillery targeted Ukrainian cellular towers, SpaceX CEO Elon Musk moved his company's Starlink satellites over Ukraine to fill the resulting communications gap.[2] This use of privately-owned property helped not only to direct military communications, but also allowed for Ukrainian citizens to broadcast their plight to the rest of the world through social media as never before. While SpaceX's decision here aligned with U.S. interests, it leaves open the question of how private interests, especially those of foreign nationals, will shape warfare in years to come through space technology.

ADDRESSING THE HYPERSONIC THREAT

Space-based assets are critical for another reason as well: utilizing them may be the only way to counter the burgeoning threat of hypersonic weapons. Hypersonic weapons employ fast missiles with substantial maneuverability, the trajectory of which can be altered during flight.[3] This class of missiles differ from ballistic missiles, which travel at similar speeds but have a predetermined trajectory that cannot be manipulated until the terminal phase of flight. Hypersonics also trump traditional cruise missiles, which have similar

Dee McHardy *and* ***Margaux Miller*** *are researchers at the American Foreign Policy Council in Washington, DC.*
Peter Garretson *is co-director of AFPC's Space Policy Initiative and co-author of The Next Space Race: A Blueprint for American Primacy (forthcoming in 2023 from Praeger).*

maneuverability during flight but travel at much slower rates of speed. Research to counter hypersonic weapons includes kill mechanisms, such as high-powered microwaves and particle-dispensing warheads, which exploit their vulnerability as a result of operating at high speed and have shown promise in interception.[4] However, any interception technology first requires knowing the path of the missile itself. Unchecked, these weapons pose a serious threat to the U.S. military, because of an inability to accurately track and respond to them.

Since hypersonic weapons fly outside the parameters of our traditional radar systems, there is now a push to develop a constellation of satellites in low Earth orbit (LEO) to track these threats.[5] The proliferation of LEO constellations is enabling a wealth of novel commercial services, but it is also driving new methods for tactical intelligence, surveillance, and reconnaissance (ISR), including low-latency missile warning and tracking. According to the Pentagon, the U.S. will launch 28 satellites into LEO to combat adversarial threats by 2025.[6] More specifically, these satellites will track the movement of missiles and predict their points of impact. Over time, the DoD's Space Development Agency plans to create a collective group of over 100 satellites in LEO to expand its coverage of threats and better prepare for defense against hypersonics.

When Russian artillery targeted Ukrainian cellular towers, SpaceX CEO Elon Musk moved his company's Starlink satellites over Ukraine to fill the resulting communications gap. … While SpaceX's decision here aligned with U.S. interests, it leaves open the question of how private interests, especially those of foreign nationals, will shape warfare in years to come through space technology.

OFFENSIVE SPACE ACTIVITIES

Significant advancements have also been made by America's adversaries in anti-satellite (ASAT) technology. ASAT weapons, if used against U.S. satellites, can cause unfathomable destruction across many industries on which the United States has become dependent, including GPS, telecommunications, and weather monitoring. This poses a clear national security vulnerability, since our economy relies heavily upon certain critical military and commercial space systems. If the functions of these systems are interrupted, the U.S. may lose internal connectivity, or connectivity with the rest of the globe.

There are currently several types of ASAT technologies, including direct ascent missiles (missiles shot toward a satellite for a kinetic impact), co-orbital satellites (satellites orbiting near the target satellite that crash into it, grab it, or spray it), jamming (preventing communication), cyber attacks on satellites or ground stations, or directed energy weapons (lasers or microwaves beamed from the ground or from other satellites). Several nations have already demonstrated the ability to target their own satellites in space with destructive ASAT tests, but countries are developing other methods of satellite attack. China, for instance, recently conducted a docking maneuver with one of their satellites that had launched earlier this year. The Shijan-21 (SJ-21) attached to the CompassG2 network satellite, functioning as a space tug.[7] This raises concerns about a future Chinese capability to latch onto satellites from other countries, removing them from their orbit or restricting their controls.

How is the U.S. responding? In April, Vice President Kamala Harris announced that the U.S. will not partake in direct-ascent ASAT missile testing.[8] The announcement followed Russia's detonation of its own satellite last year, which threatened the lives of the crew aboard the International Space Station (ISS). Harris' decision reflects the fact that the U.S. recog-

nizes the danger of debris-causing direct ascent ASAT (DA-ASAT) weapons.[9] While protecting our satellites is paramount, the debris caused by exploding enemy satellites creates dangers for all.

However, there is potential for Directed Energy Weapons (DEW) to be implemented by the Space Force as a response. According to Todd Harrison, formerly of the Center for Strategic & International Studies, a DEW "has the advantage of protecting satellites without producing space debris, which is important to the long-term viability of the space domain for all users, not just the U.S. military."[10]

Space has become an operational center of gravity for a major theater war in which both sides perceive the ability to have space enhancements and deny them to others, leading to an offense dominant and unstable regime. Given the numerous satellite attack vectors and reliance on space for national security and economic purposes, it is difficult to determine how a nation can truly protect essential space assets. These vulnerabilities could drive an ASAT arms race, as well as one to develop counter-ASAT capabilities, in the years to come.

Space has become an operational center of gravity for a major theater war in which both sides perceive the ability to have space enhancements and deny them to others, leading to an offense dominant and unstable regime. Given the numerous satellite attack vectors and reliance on space for national security and economic purposes, it is difficult to determine how a nation can truly protect essential space assets.

SPACE-BASED SOLAR POWER

In the face of rising energy insecurity, space-based solar power (SSP) stands poised to provide consistent, renewable energy on a massive scale.[11] The technology itself consists of photovoltaic satellites that convert solar energy into microwaves and wirelessly beam them to a receiver site on the ground anywhere in the world. This 24-hour solar energy collection can provide gigawatt levels of clean energy, giving the state that develops the technology massive advantages in everything from manufacturing to transportation. Once considered prohibitively expensive, recent advancements have made this technology not only feasible, but even potentially commercially cost effective.[12] SSP holds the key to both energy security and combatting climate change, while still supporting sustainable economic growth.

Militarily, SSP could support expeditionary operations or a forward operating base powering everything from refueling stations to missile radar systems. Combat vehicles and remote outposts would no longer need to rely on precarious fossil fuel supplies. Additionally, smaller military SSP satellites could power critical surveillance drones, granting them indefinite flight times without the need to refuel. SSP allows our military to become energy independent, no matter where in the world it is located.

However, the U.S. is not currently leading in the development of this technology. Here, the advantage is China's. China has had a dedicated SSP research program since 2006, and completed a successful ground test of the technology in 2018.[13] The PRC has plans to launch a small-scale test satellite in 2025, having completed a ground receiver earlier this year. The Chinese government is determined to be the pioneer of commercial scale SSP by 2050, in line with its goal of carbon neutrality by 2060.[14] Japan and the EU have similar goals.[15] By contrast, while the U.S. is the only state known to have ground and orbital test projects, our programs are tenuous.[16] Currently, DoD and Air Force Research Laboratory (AFRL) projects in SSP are not fully funded and subject to cancellation, while comparable Chinese efforts receive sustained support.

The potential dividends are enormous. The first nation-state to develop SSP will gain incredible military, economic, and geopolitical advantages. Failing to invest in this technology would be a terrible strategic and geopolitical oversight, and would massively complicate the future of warfare for the U.S.

THE NEW ARENA

Earth-facing space technology is not the only field the military needs to worry about, however. As space economies grow, competition with other nations will as well. Malign parties could occupy or blockade access to key areas, engage in sabotage, or carry out outright damage to expensive property in the contested frontier. Thus, nations have incentives to defend their commercial ventures with military might. As our private sector ventures into Cislunar space (the space under the gravitational influence of the Earth and Moon, including the Moon's surface and surrounding area), the potential for military conflict will follow.

Yet defending space beyond our own orbit presents technical complications that, as it stands, our Space Force cannot yet overcome. Navigating in Cislunar space requires calculations of the Moon's gravity, better in-situ sensors capable of navigating that vast emptiness, and autonomous systems that can handle delays and reroutings.[17] U.S. space infrastructure developers are working to build up these capabilities through the development of in-space manufacturing, Cislunar-specific space domain awareness, refueling stations, and even novel power and propulsion. And they are making progress. In the near future, infrastructure needs will be able to be met in space.[18] Mined materials from asteroids could be processed and 3D printed into usable replacement parts, powered by renewable solar or long-lasting nuclear power, all without ever returning to Earth. This rapid development of space infrastructure opens a whole new field of possibilities, and thus potential dangers. Space itself could become the site of future conflicts.

The next few decades will be critical in deciding whether space exploration will be a cooperative or a competitive international effort. The U.S.-lead Artemis Accords follow the cooperative pattern of the ISS, now aiming to put a permanent base at the Lunar South Pole.[19] In contrast, the Chinese are pushing a "long-term civil, commercial, and military strategy to explore and economically develop the Cislunar domain with the explicit aim of displacing the U.S. as the leading space power."[20] Our ability to militarily defend our satellites and other assets from Chinese interference will be critical to thwarting that strategy.

Today, a multitude of technological breakthroughs in space have the potential to drastically change the geopolitical balance on Earth. The operative question is whether the democratic model of economic competition within the rule of law will prevail, or whether, as former NASA administrator Jim Bridenstine has put it, "it will take the form of totalitarian state control."[21] The answer to that question lies with the U.S. China, after all, has repeatedly demonstrated its commitment to developing this key strategic arena. America now needs to decide whether it will.

ENDNOTES

[1] Nathan Strout, "How One US Intelligence Agency Is Supporting Ukraine," *C4ISRNET*, April 25, 2022, https://www.c4isrnet.com/intel-geoint/2022/04/25/how-one-us-intelligence-agency-is-supporting-ukraine/.

[2] Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed The War On The Ground," *Politico*, June 8 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

[3] Richard Harrison et al., "Hypersonic Weapons," American Foreign Policy Council *Strategic Primer* vol. 6 (2019), 1-13, https://www.afpc.org/uploads/documents/Hypersonic_Weapons_Primer_-_July_2019_(web).pdf.

[4] Tom Karako and Masao Dahlgren, "Complex Air Defense: Countering the Hypersonic Missile Threat," CSIS, February 7, 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220207_Karako_Complex_AirDefense.pdf?SmaHq1sva9Sk.TSlzpX-qWY72fg8PdLvA.

[5] Christopher Stone, "Hypersonic Weapons and the Case for a Space Tracking Layer," American Foreign Policy Council *Defense Technology Program Brief*, no. 21 (2020), 1-7. https://www.afpc.org/uploads/documents/De-

fense_Technology_Briefing_-_Issue_21.pdf;
[6] Lolita Baldor, "US developing satellite system to track hypersonic weapons," Associated Press, July 18, 2022, https://apnews.com/article/russia-ukraine-china-government-and-politics-78903c58bc990f-16d12a5e16475682b8
[7] Evan Gough, "A Chinese space tug just grappled a dead satellite," *Phys.org*, February 2, 2022, https://phys.org/news/2022-02-chinese-space-grappled-dead-satellite.html#:~:text=A%20Chinese%20satellite%20pulled%20a,from%20the%20Chinese%20CompassG2%20network.
[8] Bruce McClintock, "U.S. Decision on ASAT Testing a Positive Step Towards Space Sustainability," RAND, April 21, 2022, https://www.rand.org/blog/2022/04/united-states-decision-on-asat-testing-a-positive-step.html
[9] John Venable, "Russian ASAT-Test Debris Threatens International Space Station and Escalates Global Tensions," The Heritage Foundation, November 22, 2021, https://www.heritage.org/defense/report/russian-asat-test-debris-threatens-international-space-station-and-escalates-global
[10] Nathan Strout, "The Space Force wants to use directed-energy systems for space superiority," *C4ISRNET*, June 16, 2021, https://www.c4isrnet.com/battlefield-tech/space/2021/06/16/the-space-force-wants-to-use-directed-energy-weapons-for-space-superiority/
[11] Cody Retherford, "The Promise of Space-Based Solar Power," American Foreign Policy Council, *Space Policy Review*, no.1, September 2022, https://www.afpc.org/uploads/documents/Space_Policy_Review_-_issue_1_-_9.21.2022.pdf
[12] Sandra Erwin, "AFRL and Northrop Grumman Test Key Hardware for Space-Based Solar Power Experiment," *Space News*, December 21, 2021, https://spacenews.com/afrl-and-northrop-grumman-test-key-hardware-for-space-based-solar-power-experiment/
[13] Carolyn Bartholomew and Robin Cleveland, testimony before US-China Economic and Security Review Commission, April 25, 2019, https://www.uscc.gov/sites/default/files/2019-10/April%2025%202019%20Hearing%20Transcript.pdf
[14] Stephen Chen, "China Aims to Use Space-Based Solar Energy Station to Harvest Sun's Rays to Help Meet Power Needs," *South China Morning Post*, August 17, 2021, https://www.scmp.com/news/china/science/article/3145237/china-aims-use-space-based-solar-energy-station-harvest-suns
[15] Japan Aerospace Exploration Agency, "FAQ about the SSPS," n.d., https://www.kenkai.jaxa.jp/eng/research/ssps/ssps-faq.html; European Space Agency, "Space-Based Solar Power," n.d., https://www.esa.int/ESA_Multimedia/Images/2020/08/Space-based_solar_power
[16] Sandra Erwin, "On National Security | Solar Power from Space: Will It Ever Get off the Ground?" *Space News*, January 23, 2022, https://spacenews.com/on-national-security-solar-power-from-space-will-it-ever-get-off-the-ground/
[17] David Buehler et al., "Posturing Space Forces for Operations Beyond GEO," *Space Force Journal*, no. 1 (2021), https://spaceforcejournal.org/posturing-space-forces-for-operations-beyond-geo/
[18] Bradley J. Stoor, "In-Space Manufacturing: A Roadmap to the Future." Air Command and Staff College, April 2018, https://apps.dtic.mil/sti/pdfs/AD1055025.pdf
[19] Jeff Fous, "Eight Countries Sign Artemis Accords." *Space News*, October 13, 2020, https://spacenews.com/eight-countries-sign-artemis-accords/
[20] Air Force Space Command, "The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop," September 5, 2019, https://aerospace.csis.org/wp-content/uploads/2019/09/Future-of-Space-2060-v2-5-Sep.pdf
[21] Rep. Jim Bridenstine, "This Is Our Sputnik Moment," *OKGrassroots* (blog), November 7, 2016, https://okgrassroots.com/?p=642815

Biotechnology and Today's Warfighter

Tim Marler and Daniel M. Gerstein

Biotechnology has a broad and often misunderstood scope, one with significant implications for today's warfighter. In many respects, biotechnology—and the bioeconomy more broadly—is still an emerging field, and this can exacerbate the already limited understanding of their scope. Despite a 2020 National Academies of Sciences, Engineering, and Medicine study that characterized the bioeconomy as more than 5% of the U.S. gross domestic product (or $959.2 billion) in 2016,[1] it is relatively young and often ill defined. It may have far greater potential than even these impressive totals would suggest. Furthermore, just as the technology is emerging, so too are the definitions that govern these areas. Fundamentally, however, biotechnology involves the manipulation of living organisms or their components to produce useful products.[2] Meanwhile, the broader term, bioeconomy, is based on products, services, and processes derived from biological resources.[3]

In addition to an unclear definition, public awareness, understanding, and acceptance of biotechnology may sometimes be insufficient,[4 5 6] and this presents yet another confounding factor. It makes gaining attention for these issues and developing pro-active policies challenging. Policy makers may also underestimate what biotechnology entails or how important it can be. Yet, the field can provide a wide range of opportunities to the United States while also presenting challenges and risks. Mitigating these risks and capitalizing on the opportunities could provide substantial competitive advantages for the U.S.—but only if we better understand biotechnology's scope and implications.

RELEVANT TO NATIONAL SECURITY

The broad implications of and use cases for biotechnology have emerged over many decades and ultimately impact national security and the individual warfighter. With the beginning of the genomic era and the discovery of the structure of DNA, humankind has increased its understanding of, experimentation with, and employment of biotechnology in a widening range of applications. This includes opportunities for improving the human experience and developing personalized medicine. In addition, biotechnology can help improve agricultural yields and develop novel ways to feed populations. It can offer opportunities in environmental remediation and industry, using modified organisms to mitigate polluted waterways and providing substitutes for industrial materials such as concrete. Benefits also include safer and healthier foods, cleaner manufacturing, disease treatment and perhaps even obsolescence, reduction of environmental pollutants, and harnessing of scarce natural resources. Furthermore, the broader bioeconomy also covers numerous commercial sectors, including pharmaceuticals, crop production, plastics and rubbers, as well as manufacturing and more.

The same applications that can support the rapidly emerging bioeconomy can have significant benefits for national security. Using engineered biomaterials can provide capabilities for rapidly preparing cantonment areas, building structures, and monitoring the environment. Defensive capabilities and the ability to sense attacks could be a priority in addressing these concerns. Of course, the potential for weaponization of biological material, either by states or non-state actors, remains an important concern that must factor into operational planning, as such attacks could negatively impact force health protection and mission readiness.[7]

In addition, the warfighter will undoubtedly be impacted directly by biotechnology innovations, including capabilities specifically related to improving force health protection and mission readiness. Important examples of applications for improving performance encompass a variety of products that will ensure peak physical and cognitive abilities of the warfighter. Efforts to balance the human microbiome, which is important to both digestive

Tim Marler *is a senior research engineer at the nonprofit, nonpartisan RAND Corporation and a professor at the Pardee RAND Graduate School.* ***Daniel M. Gerstein*** *works at RAND and is an adjunct professor at American University. He formerly served as the undersecretary (acting) and deputy undersecretary in the Science and Technology Directorate of the Department of Homeland Security from 2011-2014.*

and mental health, will be part of these enhancements. Optimizing warfighter performance will also include enhanced abilities to sense the environment. Furthermore, advanced neural interfaces are being developed that will improve cognition and decision-making skills.

While the human performance aspects of biotechnology offer great opportunities, the possibilities for industrial applications are perhaps equally as important. Biomaterials could be used to develop new reagents for next generation explosives, harvest rare earth materials, enhance armor protection (including protection for the individual soldier), biobased construction for airfields, and develop specialized bio resins and polymers that offer increased performance in various applications.[8] As the field of biotechnology continues to expand, still more useful applications are likely to surface.

Biotechnology is inherently dual use, meaning it could be used both for legitimate and nefarious purposes.

Biotechnology is inherently dual use, however, meaning it could be used both for legitimate and nefarious purposes. While the opportunities for combatting disease, cleaning up environmental pollutants, and harnessing scarce natural resources are positive outcomes, we should also be aware of the challenges and risks such as a rogue actor developing offensive biological warfare capabilities or the weaponization of pathogens to harm fragile biological ecosystems (perhaps through the inadvertent release of a modified species into the wild).[9]

Making matters more complicated, today a growing number of organizations that directly consider biotechnology capabilities and the issues that can affect warfighters. These include the White House Office of Science and Technology Policy, the Department of Homeland Security, the Department of Defense (DoD), the Federal Bureau of Investigation, and an assortment of national labs, just to name a few. In addition, some organizations are increasingly active in the field of biotechnology, and their work can affect the warfighter indirectly—among them, the Department of Commerce, the Department of Energy, the National Institute of Health, the Department of Health and Human Services, and the Center for Disease Control. Though not comprehensive, this list demonstrates the depth and breadth of stakeholders that exist just within the federal government, and it highlights the potential risk of disparate and uncoordinated policies.

A CONFLUENCE OF FACTORS

Given the breadth of applications and the history of relevance to the warfighter, the question arises as to why there should now be increased focus on biotechnology and why might policy considerations be especially important. Simply put, a confluence of conditions imposes a new since of urgency and momentum in harnessing the field's relevance and benefits to the warfighter.

First, there is increasing competition in this arena from "near peers" like China.[10] China has spurred a significant increase in biotechnology research and development (R&D), with an anticipated increase of 7% per year between 2021 and 2025.[11] More specifically, China has made efforts to acquire international data that can facilitate assessment and control of health care for different countries,[12] not to mention potential efforts to weaponize various aspects of biological data.[13] China's strategic investments inf the U.S. are relevant as well. While the U.S. Government's Committee on Foreign Investment in the United States (CFIUS) provides a mechanism for monitoring investments that may threaten national security, its purview is incomplete. In particular, international companies that build facilities in the United States from the ground up are not subject to scrutiny. And WuXi Biologics[14] is doing just that.[15] Although the construction, associated tax base, and potential job creation can be appealing locally, the risk to national security could well go unnoticed and unregulated. Consequently, near peer competitors could gather data about U.S. technologies and citizens without being noticed.

Second, the DoD must maintain a strong biodefense program to address the risks of deliberate use of biological weapons. As biotechnology advances and proliferates, the DoD will need to keep track of how various capabilities could be used for nefarious purposes, including deliberate attacks against populations and deployed forces. For instance, despite existing international prohibitions on biowarfare, like the 1975 Biological and Toxin Weapons Convention, the United States still has questions about

the intentions of actors such as China, Russia, North Korea, and Iran, each of which has active biotechnology programs. Engaging with the international community, including international partners and allies as well as those nations with questionable programs, could help protect the U.S. against threats.

Third, the COVID-19 pandemic has demonstrated that the U.S. is not prepared for a significant biological incident. To be sure, the problem is not new. But outbreaks and pandemics over the last decade, including Ebola (2014), Zika (2016), COVID-19 (2019-present), and now monkeypox, have demonstrated the degree to which we need to reevaluate our preparedness and response capability. This need extends to the DoD as well. The March 2020 outbreak on the aircraft carrier Theodore Roosevelt highlighted the challenges of maintaining force health protection and mission readiness in the face of a large-scale biological incident.[16]

Finally, information and capabilities related to biotechnology have proliferated and are more readily available. This availability of data, technology, and capabilities (to governments and the public) has increased substantially over recent decades, and data availability in general is an increasingly prevalent factor concerning the warfighter.[17] For example, an individual's DNA, can be mapped, stored, and used to assess a variety of personal information including susceptibility to various diseases and physical endurance and strength. New tools like CRISPR have become available in some high schools, which has democratized and deskilled biotechnology, making it more available to a wider array of people at less cost.[18]

DoD must maintain a strong biodefense program to address the risks of deliberate use of biological weapons. As biotechnology advances and proliferates, the DoD will need to keep track of how various capabilities could be used for nefarious purposes, including deliberate attacks against populations and deployed forces.

GETTING AHEAD

Given this confluence of issues, now could be the time for the U.S. government to plan ahead. To begin with, a greater degree of visibility into the various biotechnology applications being developed across government departments and agencies could be helpful. A broad and common understanding of the scope of biotechnology as it relates to the warfighter could facilitate more coordinated discussions in this regard. Greater transparency and collaboration between government, industry, academic, and international partners may also be beneficial. The recent executive order and accompanying implementation strategy go a long way in addressing these issues and help provide a common baseline for discussion.[19 20]

Hierarchy and deconfliction may be necessary. Today there are overlapping and perhaps even underlapping biotechnology areas that could be addressed to ensure proper cooperation and collaboration. There may be a need to balance centralized coordination with decentralized needs within the government. Each organization that works with biotechnology faces unique challenges and needs, and thus may require unique management. However, increasing higher-level coordination could net real benefits to the agencies themselves, as well as to the warfighter.

Finally, a greater synergy with the private sector may be necessary. Industry and academia will undoubtedly drive biotechnology R&D advancements of tomorrow. Promoting and supporting these leadership efforts, including the pace of development and innovation, will provide the DoD with the "inside track" on emerging technologies and their potential applications for national security purposes. One only need consider how government support of R&D was vital to the Human Genome Project. More recently, the government and DoD played a pivotal role in the success of Operation Warp Speed for COVID-19 vaccine development and procurement, employing such authorities as the Defense Production Act and providing funding to several of the vaccine developers.

Biotechnology may be reaching a critical junction. As it continues to mature, pro-active policy becomes necessary for the federal government to leverage emerging capabilities effectively and remain competitive. Consistent

communication, coordination, and collaboration may help retain this competitiveness and support today's warfighter most effectively.

END NOTES

[1] Marcy E. Gallo, "The Bioeconomy: A Primer", *Congressional Research Service* September 19, 2022, https://crsreports.congress.gov/product/pdf/R/R46881

[2] Merriam-Webster dictionary, https://www.merriam-webster.com/dictionary/biotechnology

[3] Marcy E. Gallo, "The Bioeconomy: A Primer", *Congressional Research Service* September 19, 2022, https://crsreports.congress.gov/product/pdf/R/R46881

[4] Onyango, B., Govindasamy, R., Hallman, W. (2006), "U.S. Public Awareness and Knowledge of and Interest in Biotechnology: A Principal Component Factor Analysis," *Journal of Food Distribution Research*, 37 (1), https://ageconsearch.umn.edu/nanna/record/8577/files/37010126.pdf?withWatermark=0&version=1&registerDownload=1

[5] McHughen, A. (2007), "Public Perceptions of Biotechnology," *Biotechnology* Journal, 2, 1105-1111, https://onlinelibrary.wiley.com/doi/epdf/10.1002/biot.200700071

[6] Pauwels, E., "Public Understanding of Synthetic Biology," *BioScience*, February 1, 2013, 63 (2), https://academic.oup.com/bioscience/article/63/2/79/534322

[7] Hessel, A., Goodman, M., Kotler, S., "Hacking the President's DNA," *The Atlantic*, November 2012, https://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/

[8] Diane Dieuliis, « Biotechnology for the Battlefield: In Need of a Strategy," *War on the Rocks*, November 27, 2018, https://warontherocks.com/2018/11/biotechnology-for-the-battlefield-in-need-of-a-strategy/

[9] Tucker Davey, "Benefits and Risks of Biotechnology", **Future of Life Institute**, November 14, 2018, https://futureoflife.org/background/benefits-risks-biotechnology

[10] Carlson, R., Sbragia, C., Sixt, K. (2021), "Beyond Biological Defense: Biotech in U.S. National Security and Great Power Competition," *Institute for Defense Analysis*, https://www.ida.org/-/media/feature/publications/b/be/beyond-biological-defense-biotech-in-us-national-security-and-great-power-competition/p-22700.ashx

[11] Kharpa, A. (2021), "China Spending on Research and Development to Rise 7% per Year in Push for Major Tech Breakthroughs," *CNBC*, https://www.cnbc.com/2021/03/05/china-to-boost-research-and-development-spend-in-push-for-tech-breakthroughs.html

[12] Lynch, D.J., "Biotechnology: the US China Dispute over Genetic Data," *Financial Times*, July 31, 2017, https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe

[13] Brockmann, K., Bauer, S., Boulann, V. (2019), "Bio Plus X, Arms Control and the Convergence of Biology and Emerging Technologies," Stockholm International Pease Research Institute, https://www.sipri.org/sites/default/files/2019-03/sipri2019_bioplusx_0.pdf

[14] WuXi Biologics, https://www.wuxibiologics.com/

[15] WuXi Biologics' Biologics Production Facility Massachusetts, US, *Pharmaceutical Technology*, August 30, 2018, https://www.pharmaceutical-technology.com/projects/wuxi-biologics-worcester-facility/

[16] Navy Courtesy Story, "Navy Publishes Scientific Paper on USS Theodore Roosevelt COVID-19 Outbreak, U.S. *Department of Defense*, November 17, 2020, https://www.defense.gov/News/Feature-Stories/Story/Article/2414271/navy-publishes-scientific-paper-on-uss-theodore-roosevelt-covid-19-outbreak/

[17] Winkler, J. D., Marler, T., Posard, M., Cohen, R. S., Smith, M., "Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense," *RAND Report PE-324-OSD*, 2019, https://www.rand.org/pubs/perspectives/PE324.html

[18] Lutz, E. (2022), "CRISPR in the Classroom," *The New York Times*, https://www.nytimes.com/interactive/2022/06/27/science/crispr-anniversary-classroom-explainer.html

[19] Joseph R. Biden, Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy, September 12, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/

[20] White House, "National Biodefense Strategy and Implementation Plan", October 2022, https://whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

The Future of Wargaming

Chris Dougherty

The field and practice of wargaming has exploded in popularity in the seven years since then-Deputy Secretary of Defense Bob Work and then-Vice Chairman of the Joint Chiefs of Staff Gen. Paul Selva published their call to reinvigorate the practice in the Department of Defense and the broader defense community.[1] Their paper—and subsequent critical attention and investments—had the desired effect. But it has also created challenges in designing and executing wargames, as well as applying wargaming insights to broader campaigns of research to inform defense decisions. These challenges include: quality, repeatability, and incorporation with modeling and real-world exercises into campaigns of learning.

REVITALIZING THE DISCIPLINE

A defense analyst recently commented on Twitter that we had reached, "peak wargaming," suggesting a bubble of interest in the method that was due for a downward correction.[2] While I disagreed with the conclusion, the sentiment isn't unfounded. Work and Selva's article sparked a surge in demand for wargaming that far outstripped available supply.

Defense organizations rallied to fill this gap. Before 2015, only a handful of organizations regularly ran wargames for the Department of Defense. Internally, these included the Joint Staff's Studies, Analysis, and Gaming Division (SAGD), the Center for Army Analysis, (CAA), and the wargaming department at the Naval War College. Today, there are gaming cells or teams spread across the department (e.g., the Air Force's Agile Wargaming Team) and its research and educational institutions such as the war colleges, service academies, and the research laboratories.

A similar trend occurred outside the Pentagon. Pre-2015, among the Federally Funded Research and Development Corporations (FFRDCs), only the Center for Naval Analyses (CNA) had a full-time gaming staff. The RAND Corporation ran games as part of their research efforts, but did not have a gaming team per se. The other major FFRDCs that directly support the Pentagon, MITRE and the Institute for Defense Analyses (IDA), had no gaming capability. Today, however, CNA, RAND, and IDA all have standing wargaming programs, while MITRE is in the process of developing one.

Non-governmental research institutes (i.e., think tanks) also followed this pattern. Prior to 2014, only the Center for Strategic & Budgetary Assessments (CSBA) regularly ran wargames. Today, the Center for a New American Security (CNAS) and the Center for Strategic & International Studies (CSIS) also have wargaming teams, and the Atlantic Council, Hoover Institute, and other think tanks have started running wargames. Additionally, academic institutions including the Massachusetts Institute of Technology have started wargaming.

This growth has clearly increased the supply of wargames in the marketplace, but at the cost of quality. The decline of wargaming during the post-Cold War period and the post-9/11 wars that Work and Selva hoped to reverse created a generational gap in wargame designers, players, and analysts. Games are a fundamentally human endeavor, and their output is only as good as the people involved.[3] A variety of efforts are underway to fill this gap, however, and if properly executed, could spawn sustainable innovation in wargaming. The Military Operations Research Society (MORS), for example, has multiple programs to develop wargamers. Georgetown University's Security Studies Program, the Johns Hopkins School of Advanced International Studies, and George Washington University's Elliot School of Foreign Affairs also have

Chris Dougherty *is a Senior Fellow for the Defense Program at the Center for a New American Security (CNAS). His primary areas of research include defense strategy, operational concepts, and force planning. Previously, he served as senior advisor to the deputy assistant secretary of defense for strategy and force development at the Department of Defense.*

wargaming coursework and clubs. Sebastian Bae, a wargamer at CNA and a former Marine, recently edited a book on this topic, *Forging Wargamers: a Framework for Wargaming Education.*[4]

These initiatives are developing a new generation of game designers and players who are bringing enthusiasm and new perspectives to a field that needs both. Like past generations of wargamers, many of these new recruits started as hobby gamers. Unlike the previous generation that became interested in wargaming during the heyday of traditional "hex and counter" wargames in the 1970s and 1980s, this new generation is more familiar with computer strategy games, "Euro-style" boardgames like "Settlers of Catan," and card-driven games like "Magic: the Gathering."[5] This familiarity with different media and methods is breaking down barriers and driving innovation.

Wargames, it must be clear, are not computer models, nor should they attempt to replicate them. The richness of gaming comes from exploring human decision-making in competitive and uncertain situations.

RAND's "Hedgemony" is a good example of this innovation (full disclosure, the author sponsored development of Hedgemony while serving in the Pentagon to support the 2018 National Defense Strategy).[6] Hedgemony is defense strategy game designed to look, feel, and play like a Euro-style board game. It has pieces, cards, a point tracker, and "victory" conditions. Its board-game feel allows it to educate laypeople about defense strategy while its analytic rigor allows it to inform major strategic decisions. Tim Barrick's "Operational Wargaming System" and Sebastian Bae et al.'s "Littoral Commander" are two further examples of innovative wargame design.[7]

"Hedgemony," the "Operational Wargaming System," and "Littoral Commander" also share another key feature: they are repeatable. Professional wargames have historically used bespoke or nearly bespoke designs. This enables designers to develop and run games that are specific to a particular problem. The downside of this approach is that it is time- and resource-intensive, and it limits the broader applicability of a game and any data or insights that it generates. "Hedgemony," by contrast, was designed specifically to be played repeatedly at low cost to allow for exploration of different strategic futures and assumptions. This decision limited the flexibility of the design, but the benefits in terms of playability and data capture for analysis were well worth it.

NETWORKING DATA

Data capture and analysis are the next frontier for wargaming. Deputy Secretary of Defense Kathleen Hicks and others are now striving to turn the Department of Defense into a data-driven organization that can leverage "big data" and artificial intelligence (AI) to make better decisions. The reality, however, is that most wargames do not capture or use data in ways that support this vision. This shortfall in data management reinforces unhelpful cultural schisms in the defense community between qualitatively minded wargamers and quantitatively minded operations researchers and modelers. Wargames, it must be clear, are not computer models, nor should they attempt to replicate them. The richness of gaming comes from exploring human decision-making in competitive and uncertain situations. That doesn't mean, however, that games—provided they deal ethically with researching human subjects—cannot capture good data for follow-on analysis. Indeed, if wargaming is going to survive in a data- and AI-driven future, this is as much a necessity as an opportunity.

This future vision is best captured by BrainSTORM, which is the work of Dr. Alec Barker et al., and won the prestigious Barchi Prize in 2021.[8] BrainSTORM, which was sponsored by the Defense Advanced Research Projects Agency (DARPA), took the Defense Department's most credible joint campaign model, the Synthetic Theater Research Operations Model, or STORM, and turned it into a simple online wargame.

Data capture and analysis are the next frontier for wargaming. Deputy Secretary of Defense Kathleen Hicks and others are now striving to turn the Department of Defense into a data-driven organization that can leverage "big data" and artificial intelligence (AI) to make better decisions. The reality, however, is that most wargames do not capture or use data in ways that support this vision.

This crossover between wargaming and modeling would have been interesting on its own, but the team also developed sophisticated AI that could "play" BrainSTORM and act as an advisor to players in a version of "centaur" wargaming.[9]

BrainSTORM is the bellwether of a future in which wargames use transparent and automated tools for adjudication and data capture. Like BrainSTORM, these games could use AI to advise players on different courses of action during gameplay, or use AI and underlying model for robust and credible post-game analysis. The beauty of this vision is two-fold. First, it combines the best of wargames (human interaction) and models (rigor and data capture). Second, it would enable incorporation with emerging technologies in training and exercises to create a rapid "cycle of research."

First described Peter Perla, the dean of modern wargaming, a cycle of research includes wargaming, quantitative analysis and modeling, and real-world exercises.[10] Though sometimes described as a linear process, Perla's vision was more a complex interaction between three different methodologies, with each providing its unique contribution.[11] Unfortunately, as alluded to above, wargaming and analysis/modeling have a fraught relationship.

There are neither robust relationships between the organizations that conduct wargames and analysis and those that conduct exercises, nor are there shared data standards or frameworks for understanding that data. The result is that the cycle of research is instead three stovepipes of learning operating in parallel. Insights derived from wargames are not examined using models to determine their robustness. Models lack insights from wargames and instead make assumptions about human behavior and decisions. Both methods lack a real-world check on their assumptions and insights. Likewise, real-world exercises often seem detached from the wargames and analysis occurring inside the department.

BrainSTORM demonstrated that wargames and models can coexist and act synergistically. Closing the loop on a truly interactive cycle of research requires incorporating training and exercises through the use of live, virtual, and constructive (LVC) training.[12] LVC training can provide a real-world but data-driven check on insights from wargames and models that, by their nature, are wholly simulated.

THE WAY FORWARD

From the challenges facing wargaming today—quality, repeatability, and incorporation with modeling and exercises into a cycle of research—we can begin to see a tentative vision for the future of defense wargaming and analysis. A new, younger cadre of wargamers pushing boundaries to develop innovative and repeatable wargames that iterate closely with computer models and LVC training to generate vast quantities of data for analysis, training, and education. This future isn't quite here today, and there are obstacles. Traditionally fractious bureaucracies will need to agree on methods, models, algorithms, and data standards, knowing full well that these agreements will heavily influence future analysis and with it the shape of the future force.

If the Pentagon and defense community can hurdle these obstacles, however, there is an immense opportunity to exploit the full potential of wargaming in campaigns of research that improve the ability of U.S. and allied forces to compete with, deter, and if necessary, defeat Chinese or Russian aggression.

END NOTES

[1] Bob Work & Paul Selva, "Revitalizing Wargaming is Necessary to be Prepared for Future Wars," *War On The Rocks*, December 8, 2015, https://warontherocks.com/2015/12/revitalizing-wargaming-is-necessary-to-be-prepared-for-future-wars/.

[2] Christopher M. Dougherty [@C_M_Dougherty], "I don't think we've reached peak wargaming, so much as we've reached a point where demand far outstrips quality supply. We need more experienced designers, more good red teamers, & more rigorous back end analysis & incorporation w/other methods," Tweet. Twitter, August 21, 2022, https://twitter.com/C_M_Dougherty/status/1561331203050987526.

[3] Christopher Dougherty, "It's Time to Rethink our Wargames," *Inkstick*, May 13, 2020, https://inkstickmedia.com/its-time-to-rethink-our-wargames/.

[4] Sebastian J. Bae, *Forging Wargamers* (Virginia, Marine Corp University Press, 2022), https://www.usmcu.edu/Portals/218/Forging%20Wargamers_web.pdf.

[5] Jonathan Kay, "The Invasion of the German Board Games," *The Atlantic*, January 21, 2018, https://www.theatlantic.com/business/archive/2018/01/german-board-games-catan/550826/.

[6] Michael E. Linick, John Yurchak, Michael Spirtas, Stephen Dalzell, Yuna Huh Wong, and Yvonne K. Crane, *Hedgemony: A Game of Strategic Choices* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/tools/TL301.html.

[7] Wargaming Division Staff, "An Invigorated Approach to Wargaming," *Marine Corp Gazette*, February 2020, pg. 21, https://mca-marines.org/wp-content/uploads/An-Invigorated-Approach-to-Wargaming.pdf; Rex Brynen, "Dietz Foundation: Littoral Commander," *PAXsims*, 30 January, 2022, https://paxsims.wordpress.com/2022/01/30/dietz-foundation-littoral-commander/.

[8] Alec Barker, "BrainSTORM: exploring artificially intelligent COA development in STORM," presentation at the SPIE Defense + Commercial Sensing Proceedings 11746, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, online, April 12, 2021, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11746/1174605/BrainSTORM-exploring-artificially-intelligent-COA-development-in-STORM/10.1117/12.2587186.short?SSO=1

[9] Mike Cassidy, "Centaur Chess Shows Power of Teaming Human and Machine," *Huffington Post*, December 30, 2014, https://www.huffpost.com/entry/centaur-chess-shows-power_b_6383606.

[10] Peter P. Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Maryland, Naval Institute Press, 1990).

[11] Peter P. Perla, Web Ewell, Christopher Ma, Justin Peachy, Jeremy Sepinsky, and Basil Tripsas, "Rolling the Iron Dice, from Analytical Wargaming to the Cycle of Research," *War On The Rocks*, October 21, 2019, https://warontherocks.com/2019/10/rolling-the-iron-dice-from-analytical-wargaming-to-the-cycle-of-research/.

[12] Jennifer McArdle and Caitlin Dohrman, "The Next Simnet? Unlocking the Future of Military Readiness Through Synthetic Environments," *War On The Rocks*, December 3, 2020, https://warontherocks.com/2020/12/the-next-simnet-unlocking-the-future-of-military-readiness-through-synthetic-environments/.

The Future of Defense Learning and Development

Sae Schatz

The Defense workforce carries a heavy burden. It's expected to operate across all phases of competition and perform an expanded set of missions (from traditional engagements to counterinsurgency, cybersecurity, civil affairs, battlefield medicine, humanitarian assistance, and so on). It needs to possess the independent decision-making skills to operate on intent, balance tactical actions against strategic effects, and apply complex skills within a joint, interagency, intergovernmental, and multinational context.

Put another way, today's Department of Defense (DoD) workforce is expected to develop a broader and more sophisticated set of capabilities than any previous generation—and do so in the same (or even less) time as before. It's also expected to continuously learn, adapt, and grow as new technologies emerge and the volatile global environment shifts. Yet our conventional training and education methods aren't well-suited to these challenges. Consequently, across DoD, organizations are evolving their learning and development approaches.

THE MOTHER OF INVENTION

This demand for reform is echoed throughout DoD policy and Congressional legislation, including recent documents like the 2022 *National Defense Authorization Act*, the 2022 *National Defense Strategy*, the Army's *Learning Concept for 2020–2040*, the Navy's *Ready, Relevant Learning,* the Air Force's *Strategic Master Plan Human Capital Annex,* the Marine Corps' *Training and Education Command (TECOM) Strategy 2020–2030,* and the Space Force's *Guardian Ideal*. Looking back a bit further, similar calls were made by then-Secretary of Defense Ash Carter and the Force of the Future reform led by the Office of the Under Secretary of Defense for Personnel and Readiness under his tenure. Retired General Martin Dempsey, then-commander of the Army's Training and Doctrine Command (TRADOC), also called for "a Campaign of Learning" in 2010, and the Marine Corps released a series of plans in 2008 that led TECOM to explore *Small Unit Decision Making* and *Instructor Professionalization* projects.[1]

Although the antecedents began nearly two decades ago, DoD has reached a tipping point in terms of organizational support for reform and the external pressures necessitating it. These changes have taken the form of at least six specific trends:

1. Increased use of online learning

Like the rest of the world, the pandemic pushed DoD to move more of its training and education online. This is largely a good thing. Online learning is vastly more affordable in terms of both time and money,[2] and research has firmly established that it's as good as—if not better than—conventional classroom methods.[3] DoD's scale means it can greatly benefit from the resource incentives, and over the last two years DoD (and even organizations in the intelligence community) have shown they can safely shift many courses online.

To be effective, though, e-courses need to be welldesigned. Learners need to be held accountable for learning, not simply copying answers from internet discussion boards or outright cheating. And individuals need dedicated time to learn without frequent interruptions or relegating their studies to nights and weekends. So, although e-learning is a proven approach and DoD has shown it can migrate coursework online, broad organizational changes are still needed to use e-learning most effectively in practice.

2. Integration of new technologies

The ed-tech market is exploding with new possibilities. A few popular trends include microlearning (delivering content in 1–15 minutes chunks, often via a smartphone

Sae Schatz, PhD *is co-founder of Bedrock Learning, Inc. and formerly the director of DoD's Advanced Distributed Learning (ADL) Initiative. She's an expert at the intersection of digital, data, and talent modernization. Find her online at LinkedIn or @SaeSchatz on Twitter.*

app), adaptive learning (also called intelligent tutors; AI-enabled systems that adjust to learners' characteristics or performance), and mixed reality (also called XR, which spans the continuum of virtual to augmented reality). Some of these technologies offer notable benefits. For example, DARPA sponsored a famous intelligent tutor to train IT professionals.[4] It produced remarkable effect sizes up to 3–4σ,[5] and its learners outperformed seasoned Navy professionals after only 16 weeks of training.

However, despite ed-tech's promise, many new systems fail to live up to their hype because they ignore core principles. For instance, new technologies may lack a strong pedagogical[6] foundation, or they may be employed in old ways—simply substituted for an analog component in an outdated system. In other words, to be effective, new technologies require systematic organizational change and thoughtful implementation by experts skilled in learning science, not only IT administration.

Although e-learning is a proven approach and DoD has shown it can migrate coursework online, broad organizational changes are still needed to use e-learning most effectively in practice.

3. An emphasis on outcomes—especially competencies

Learning is most effective when outcomes are assessed and learners are held accountable to reaching those goals, while allowing time on task and instructional methods to vary. This approach is called mastery learning. It stands in contrast to settings where factors like classroom time or teaching methods are constant, and individuals' performance varies. The Joint Staff recently updated the *Officer Professional Military Education Policy* (CJCSI 1800.01F), shifting its requirements from process- to outcomes-focused. Similarly, the Under Secretary for Personnel and Readiness just signed the inaugural Military Education policy (DoDI 1322.35), which emphasizes outcomes-based military education and makes a nod toward the more advanced competency-based approach.

Competencies are the patterns of knowledge, skills, abilities, behaviors, and other characteristics needed to successfully perform a role or task. They're usually defined as observable indicators at different levels of mastery (e.g., novice, intermediate, advanced). Using a competency-based approach not only improves achievement; it can also serve as a Rosetta Stone to align learning, employment, and personnel data across organizations. For these reasons, the Services have begun releasing policy directing the use of competency-based approaches, including the Air Force's *Competency Modeling* (2022), the USMC's *TECOM Strategy 2020–2030*, and Space Force's *Guardian Ideal*.

Implementing a competency-based approach may be difficult for DoD to achieve, however. Doing so properly requires a combination of technical skill (to implement the enterprise data systems and accurately define each node's characteristics) and organizational change (to transform training, education, and employment paradigms). Additionally, DoD needs strong, central leadership to build a department-wide approach and common frameworks. Without these, the Department will squander the opportunity for interorganizational interoperability and limit its ability to realize enterprise-scale learning innovations (see #6 below).

4. Creative ways to estimate capability

Assessments are a quintessential part of training and education. They come in various familiar forms, like quizzes and observer/trainer checklists, but these aren't the only ways to estimate individual or team capabilities. Professor Valerie Shute, for example, popularized the concept of "stealth assessment," which interweaves evidence-collection directly and invisibly into an application environment. In a series of studies, Shute and her colleagues were able to infer individuals' skills, such as problem-solving ability, simply via their interactions in the popular video game *Plants vs. Zombies 2*.[7] Other emerging evaluation methods include hardware sensors (e.g., brain-monitoring EEGs, eye trackers, and position sensors), emotion recognition through camera inputs, mouse and keyboard clickstreams, and data fused from multiple sources.

There are increasingly numerous ways to collect evidence, albeit largely thanks to advancements in

sensor technologies, AI, and interoperability. Still, those advancements are inconsequential for learning contexts without corresponding investments in reliable, valid measures and learning analytics methods.[8] DoD organizations, such as those participating the Personalized Assessment, Education, and Training subdivision under DoD's Human Systems Community of Interest have invested decades of research into relevant methods, and it's important that their quiet, nuance work is integrated with the showier technology components.

To be effective, new technologies require systematic organizational change and thoughtful implementation by experts skilled in learning science, not only IT administration.

5. Acceptance of credentials and micro-credentials

Credentials are qualifications (such as diplomas, certificates, or licenses) granted by an authoritative body like a university or industry association. They're best paired with a competency-based approach as indicators of accomplishment against defined competencies. Credentials can reflect large or small achievements, but the latest trend is to award micro-credentials (also called nano-degrees or digital badges). These are often stackable, so that completing a series earns a larger credential like a certificate or bachelor's degree.

Micro-credentials are typically personalized, allowing individuals to mix-and-match across a set of stackable options, available *flexibly* (including on-demand online), and *shareable* in the form of digital tokens. Case studies demonstrate that these features improve access to education for lower income students[9] and help close the opportunity gap. For DoD, this approach could also help offload some of its swelling learning and development requirements, aid interorganizational and interagency permeability, and improve learning personalization.

Current DoD systems adequately manage credentials earned within the agency, with efforts such as DoD's Credentialing Opportunities On-Line (COOL) and DoD Instruction 1322.33 ("DoD Credentialing Programs") opening the door to limited external credentials. Still, notable policy and process reforms are needed before the Pentagon can reliably accept credentials from external organizations and treat them equivalently to conventional markers of achievement like four-year degrees or time in grade.

6. Progress toward the "Learning Ecosystem" approach

There's a growing movement to comprehensively evolve the classical model of training and education. A learning ecosystem is a system of systems comprised of interconnected technologies that operate cohesively through interoperable interfaces and data interchange. The idea is for an individuals' *lifelong* learning to be personalized across their everchanging contexts, goals, areas of study, and personal characteristics. That is, for individuals to have access to optimized learning experiences—delivered when and how they're needed—throughout their lives, whether those experiences be a multiyear educational program on military strategy or an on-demand XR micro-trainer on engine repair.

Several sources have popularized this concept, including a book from DoD's Advanced Distributed Learning (ADL) called *Modernizing Learning: Building the Future Learning Ecosystem*,[10] Harvard's 60-Year Curriculum,[11] and the learning engineering movement championed by IEEE's Industry Consortium on Learning Engineering.[12] DoD is also making progress toward this vision via its Enterprise Digital Learning Modernization reform as well as Service-level efforts like MyNavy Learning, MarineNet Ecosystem, Air Force's myLearning, and various Defense Acquisition University DAUx projects.[13]

Fully achieving the learning ecosystem approach will require sweeping enterprise data modernization, new learning engineering methods, updates to instructional technologies, and new processes for DoD talent development—if not talent management, overall. These steps, however, can be taken incrementally, and each of the trends described above is part of the solution.

The learning ecosystem approach is, in part, a realiza-

tion of the human domain portion of Joint All-Domain Command and Control (JADC2)—DoD's strategy to achieve victory through data and interconnected technologies. In fact, "Human Enterprise" is one of JADC2's five lines of effort, and many learning ecosystem components dovetail with it.[14] Like JADC2 more broadly, the learning ecosystem approach represents an ambitious integration of many other advancements, with data at its center.

Also like JADC2, the learning ecosystem concept was crafted out of necessity, to meet the growing demands of our volatile, complex world. The learning ecosystem and other reforms described in this article aren't mere "nice to haves." They're critical advancements necessary to maintain overmatch. Learning and development transformation is an obvious way to upgrade the Total Force, but true change—not merely more resources—is needed to realize the desired benefits.

END NOTES

[1] For a useful summary, see Elaine M. Raybourn, Sae Schatz, Jennifer Vogel-Walcutt and Kendy Vierling, "At the tipping point: Learning science and technology as key strategic enablers for the future of defense and security," In *Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC)* (Washington, DC: NTSA, 2017).

[2] Stephen Maloney et al., "A cost-effectiveness analysis of blended versus face-to-face delivery of evidence-based medicine to medical students," *Journal of Medical Internet Research* vol. 17, iss. 7, 2015.

[3] Department of Education, Office of Planning, Evaluation, and Policy Development, *Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies* (Washington, DC, 2010).

[4] J.D. Fletcher and John E. Morrison, *Accelerating development of expertise: A digital tutor for navy technical training* (Alexandria, VA: Institute for Defense Analyses, 2014).

[5] The Department of Education considers effect sizes of 0.25 or higher to be of substantive importance. So, these outcomes are massive! As a comparison, effect sizes over 1σ roughly equate to an increase of learner performance from the 50th to the 84th percentile, and effect sizes over 2σ are like an increase from the 50th to the 98th percentile.

[6] *Pedagogy* refers to the knowledge and skills of teaching as well as the associated instructional methods. Educational scholars sometimes distinguish *pedagogy* (for younger learners) and *andragogy* (for mature learners), but for our purposes, the takeaway is instructional methods are critically important. Quality pedagogy has a direct, positive impact on learning outcomes—even when accounting for subject-matter expertise. There's also a linear relationship between exposure to a good—or poor—quality teacher and students' lifelong income.

[7] Valerie Shute and Matthew Ventura, *Stealth assessment: Measuring and supporting learning in video games* (Boston, MA: MIT Press, 2013).

[8] For a short academic op-ed about measurement in learning, see Sae Schatz and JJ Walcutt, "Modeling what matters: AI and the future of defense learning," *Journal of Defense Modeling and Simulation*, vol. 19, iss. 2, 2022, 129–131, https://doi.org/10.1177/15485129221088718.

[9] Justin Bariso, "How Google's new career certificates could disrupt the college degree," *Inc.*, 2021, https://www.inc.com/justin-bariso/inside-googles-plan-to-disrupt-college-degree-exclusive.html.

[10] JJ Walcutt and Sae Schatz, eds. *Modernizing learning: Building the future learning ecosystem* (Washington, DC: Government Publishing Office, 2019). https://adlnet.gov/publications/2019/04/modernizing-learning.

[11] For example, see John Richards and Chris Dede, "The 60-year curriculum: A strategic response to a crisis," *EDUCAUSE Review* vol. 55, iss. 4, October 26, 2020, https://er.educause.edu/articles/2020/10/the-60-year-curriculum-a-strategic-response-to-a-crisis.

[12] "What is ICICLE?" IEEE, n.d., https://sagroups.ieee.org/icicle.

[13] For DoD future learning ecosystem examples, see ADL Initiative, *Defense ADL Advisory Committee (DADLAC) Annual Report 2021* (Washington, DC, 2022), https://apps.dtic.mil/sti/pdfs/AD1158349.pdf.

[14] Department of Defense, *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

Ilan Berman	Chief Editor
Richard Harrison	Managing Editor
Rehna Sheth	Graphic Design and Layout

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the *Defense Dossier* (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

ABOUT THE AMERICAN FOREIGN POLICY COUNCIL

For four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.