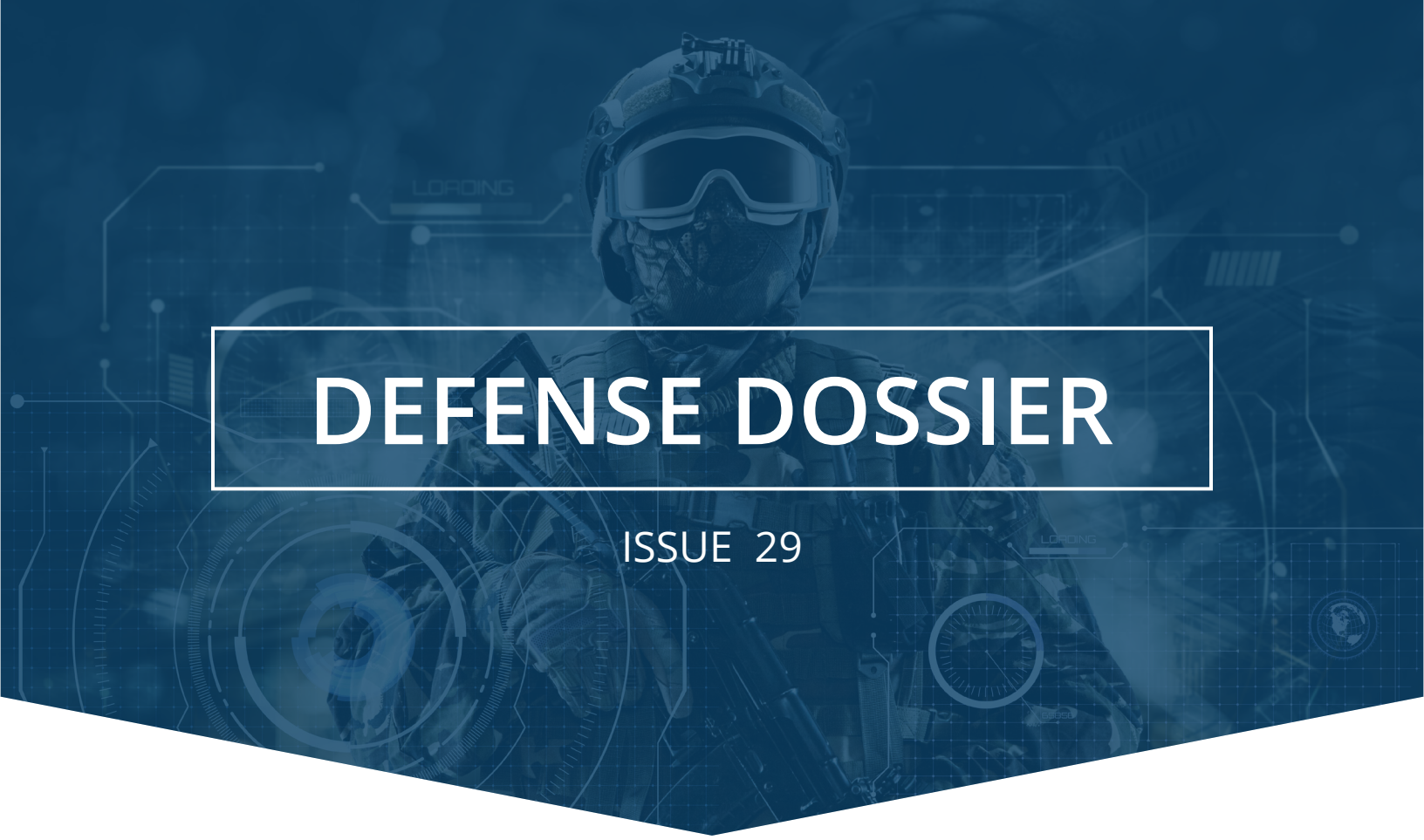


DEFENSE DOSSIER

ISSUE 29

DECEMBER 2020

AFPC

AMERICAN FOREIGN POLICY COUNCIL

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

DEFENSE DOSSIER

DECEMBER 2020 | ISSUE 29

LETTER FROM THE EDITORS

Welcome to the December 2020 edition of the American Foreign Policy Council's *Defense Dossier* e-journal.

In this edition of the *Dossier*, we take a closer look at the future of warfare in its various permutations. From quantum technology to the increasingly intertwined fields of electronic warfare and cybersecurity, as well as advances in drone technology and nuclear energy systems, today's battlefield is being reshaped in profound ways – and American defense priorities are changing along with it. At the same time, new challenges (such as developing truly "trusted" artificial intelligence) will test the adaptability and flexibility of American defense planners like never before.

The articles in this collection provide a glimpse at the breakthroughs and barriers that the U.S. military will face in the years ahead—and offer some ideas about how the U.S. government can best adapt to them. They are problems and opportunities well worth thinking about as the United States navigates a rapidly changing modern battlefield.

Sincerely,

Ilan Berman
Chief Editor

Richard M. Harrison
Managing Editor

The Promise and Peril of Quantum Technology

Richard M. Harrison

On October 23, 2019, tech giant Google made a shocking announcement. Using the pages of the prestigious *Nature* magazine as a platform, the company declared that its *Sycamore* quantum computer had achieved "quantum supremacy."[1] Renowned theoretical physicist John Preskill had coined the term "quantum supremacy" to delineate a time when quantum computers could solve a problem or task not easily achievable by a classical computer.[2] Google claimed that its quantum supercomputer had one that, successfully completing a calculation in 200 seconds that it would take a classical computer 10,000 years to complete.[3]

In response, IBM argued that its nonquantum supercomputer could make the same calculation in just a few days,[4] but the milestone was nonetheless undeniable. The quantum revolution had just taken a major step forward. In the years ahead, the effects will reverberate across numerous sectors, from banking to cybersecurity to logistics and transportation.[5] A principal focus for U.S. policymakers, however, will be the impact of quantum technologies on U.S. national security and military affairs.

WHAT IS QUANTUM TECHNOLOGY?

Quantum technologies operate at the subatomic scale and, in the simplest terms, are governed by the principles of "superposition" and "entanglement." Entanglement refers to the property where two particles are linked, so that when one particle is measured it uncovers the state of the other particle—even over long distances with no physical connection.[6] For example, if a coin is spinning in New York and another linked identical coin is spinning in Beijing, if one coin is stopped then the other coin will halt as well, and display an identical face.[7]

The principle of superposition states that, while unobserved, a particle is able to reside in multiple states simultaneously.[8] This property is in direct contravention to classical physics, which posits that a particle can only exist in one state at any given time. For example, in classical computing data is stored in binary fashion with a bit (basic data unit) equaling a 1 or a 0. In quantum computing, however, a qubit (such as a photon, atom, etc.) is able to be both a 1 and 0 simultaneously.[9] Thus, "Two bits in a classical computer provides four possible combinations—00, 01, 11, and 10, but only one combination at a time. Two bits in a quantum computer provides for the same four possibilities, but, because of superposition, the qubits can represent all four states at the same time, making the quantum computer four times as powerful as the classical computer. So, adding a bit to a classical computer increases its power linearly, but adding a qubit to a quantum computer increases its power exponentially—doubling power with the addition of each qubit."[10] Superposition of particles and simultaneous calculation leads to lightning fast analytical ability, which allows quantum computers to excel at optimization problems. For example, unlike a classic computer, in a game of chess a quantum computer would be able to immediately analyze the outcome of all possible scenarios, and choose the optimal solution.[11]

While quantum computing receives the most media attention, the broader sector of quantum information sciences (QIS) actually encompass three fields: quantum computing, quantum communications, and sensing and metrology. (A brief description and summary of each is provided in Figure 1).

Richard M. Harrison *is Vice President of Operations and Director of Defense Technology Programs at the American Foreign Policy Council in Washington, D.C.*

Figure 1: Quantum Information Sciences	
Quantum computing	**What it is:** Quantum computers are new machines that leverage quantum principles to compute complex problems exponentially more quickly than do existing computers.
	What it means: The ability of quantum computers to solve complex optimization problems can help ease many existing national security problems, from logistics/flow to theater optimization and wargaming. Longer-term potential benefits could include opening new frontiers for technology, improving artificial intelligence, and leading to new discoveries in science. However, the use of quantum computers will also likely require the development of new encryption techniques, as many existing ones may be vulnerable to algorithms run on quantum computers.
Quantum communications	**What it is:** In quantum communications, quantum principles are applied to create new forms of communication systems as well as new methods for securing communications. Quantum communications technology such as QKD (secure communication utilizing quantum mechanics) is one of the most mature quantum information technologies in use today.
	What it means: Most immediate uses will focus on using QKD and other methods to secure sensitive government communications such as those in nuclear command and control, but long-term uses may center on the creation of networks of quantum computers.
Quantum sensing and metrology	**What it is:** Quantum measurements leverage the highly precise manipulation of particles to detect minute changes in information.
	What it means: Quantum metrology can help create new forms of cameras, radars, and other systems. These can provide more capable means of detecting everything from stealth aircraft (quantum radar) to submarines (quantum ghost imaging) to underground facilities (quantum gravimetry). Quantum metrology can also help solve many of today's most pressing defense problems by offering new forms of location and timing not reliant on GPS signals, which can be easily jammed or spoofed.
Source: *Content drawn from Deloitte Insights'* The realist's guide to quantum technology and national security[12]	

MILITARY APPLICATIONS OF QUANTUM TECHNOLOGY

The three QIS fields outlined above have potential applications for a wide range of use in military affairs. *Quantum Computing.* The boundless processing power that future quantum computers have to offer provides the U.S. Department of Defense (DoD) with an opportunity to tackle large complex problems. One area of interest to both the DoD and intelligence community is the field of cryptology. Since quantum computers are able to carry out so many operations simultaneously, they make it feasible to crack encryption that would take classical computers years to decipher. Additionally, there is real potential for substantially improved modeling and simulation, signal processing, and applications of artificial intelligence.[13]

Quantum Communications. The characteristics of entanglement and superposition provide the DoD with a means to develop unhackable communication networks that can securely transmit classified information and alert communicating parties of any information interception attempt using the method of quantum key distribution (QKD). According to the U.S. National Security Agency, quantum key distribution "utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying

material using special purpose technology."[14] The agency further notes that QKD permits intruder detection that is not possible with standard cryptography. Furthermore, the cybersecurity benefits of quantum communication include the possibility of creating a more secure quantum internet, which could reduce the opportunities for hackers to enter critical government networks.[15] Currently, the Department of Energy is coordinating with 17 of the country's national laboratories to construct a quantum internet to securely transmit data—an effort which, if successful, could be scaled to support the private sector as well. Argonne National Laboratory in Chicago, for instance, has already demonstrated this proof of concept with a 52 mile "quantum loop."[16]

Quantum Sensing and Metrology. Of the three QIS fields, quantum sensing is arguably the most mature. Quantum sensing is not theoretical, as some quantum sensors have already proven they are more advanced than traditional sensing systems for DoD initiatives in lab testing. In a recent example, U.S. Army researchers created small and nearly undetectable quantum sensing receivers capable of identifying signals throughout the entire radio frequency spectrum.[17] A recent Congressional Research Service report provided an extensive list of uses for quantum sensing and metrology, including, "navigation, atomic clocks, gravimeters and gravitational gradiometers, inertial motion units, atomic magnetometers, electron microscopes, technologies to locate subterranean mineral deposits, and quantum-assisted nuclear spin imaging devices."[18] One of the most practical applications, however, would be during military missions in which traditional GPS is unavailable, because quantum sensors are able to provide guidance for land and sea navigation.[19] Moreover, in the future, researchers believe it may be possible to utilize entangled particles of light to detect stealth technologies using quantum sensors that are protected from radar jamming.[20]

One of the most practical quantum technology applications would be during military missions in which traditional GPS is unavailable, because quantum sensors are able to provide guidance for land and sea navigation. Moreover, in the future, researchers believe it may be possible to utilize entangled particles of light to detect stealth technologies using quantum sensors that are protected from radar jamming.

MATURING ADVERSARY TECHNOLOGY

America, however, is not the only nation focused on developing competence in quantum technology. Nor is it necessarily the leader in all QIS fields at the moment. There are a number of other countries currently investing in quantum, but the People's Republic of China (PRC) has emerged as the clear leader in terms of both capabilities and monetary investments. The PRC clearly plans to rely on quantum technology in order to achieve its strategic objective of becoming the world's premier science and technology superpower.[21] To that end, Beijing has committed considerable resources (an estimated $244 million annually) to ensure continued development of quantum technology, has established a QIS research center, and is actively targeting and recruiting experts globally.[22]

The People's Republic of China (PRC) plans to rely on quantum technology in order to achieve its strategic objective of becoming the world's premier science and technology superpower. To that end, Beijing has committed considerable resources (an estimated $244 million annually) to ensure continued development of quantum technology, has established a QIS research center, and is actively targeting and recruiting experts globally.

The PRC has also racked up a number of impressive successes in the quantum arena, including: "(1) the launch of the world's first quantum satellite, Micius, in August 2016; (2) the launch of a long-distance quantum communication landline, between Beijing and Shanghai, in September 2017; and (3) the first long-distance quantum videoconference, between the Chinese Academy of Sciences in Beijing and the Austrian Academy of Sciences in Vienna, in January 2018."[23] Additionally, China now has an operational 1,200 mile quantum loop network that dwarfs the aforementioned Argonne loop, and connects the cities of Beijing, Hefei, Jinan, and Shanghai.[24] As the PRC increasingly transitions to a quantum network for communications, it could severely complicate U.S. intelligence gathering operations. Likewise, if China continues investments in quantum sensing, it may serve to invalidate American investments in stealth technology.[25]

UNDERSTANDING THE LIMITATIONS

While the quantum revolution is underway, it is important to understand the limitations and hurdles that need to be overcome before the technology becomes a truly game-changing one.

For instance, today's quantum computers operate using tens of qubits, but a general use quantum computer is thought to need 100,000 qubits.[26] Building a computer with that type of architecture is exceedingly difficult to accomplish, as qubits need to operate at near absolute zero temperature.[27] In addition to the strict temperature constraints, qubits are inherently unstable and the tiniest vibration could disable superposition.[28] And although quantum communications have taken significant strides forward due to QKD and improvements in fiber optic links, there are limitations to the distance the quantum communication can travel (this includes the links sent via satellite by the Chinese, because they are not entirely quantum based).[29]

In general, more research is also required to understand how entanglement across long distances affects the speed and security of quantum communications.[30] Interestingly, the DoD is also not particularly concerned about Chinese progress in quantum communication, because the weakest link in security systems is the human operator, so there will always be an exploitable insider threat.[31] Finally, additional research in material science will be needed to improve the precision of quantum sensor systems.[32]

MAINTAINING MOMENTUM

The U.S. government has rightly recognized the significance and potential of quantum technology, and has pursued several initiatives intended to foster continued development. Both Presidents Obama and

Trump issued Executive Orders directing the Federal bureaucracy to formulate a QIS strategy; Congress passed The National Quantum Initiative Act (NQI Act), which coordinates research across civilian, defense, and intelligence sectors; and in August of 2020 the White House announced that the Department of Energy will be contributing $625 million over five years to establish QIS development centers overseen by national labs to spur innovation (with the private sector making a $300 million contribution to cement a private-public partnership).[33] In addition to committing funding for quantum initiatives, the 116th Congress also drafted several pieces of legislation that prevent exportation of quantum-related technology to China, in order to limit adversarial advances in QIS.[34]

In a study by the Institute for Defense Analyses, researchers recommended "that DoD support for quantum information continue, although in a focused manner to heavily support those areas where applications important for the DoD have been identified or where some key capability is envisioned."[35] "Some specific areas that we feel are particularly important," the authors noted, "are those for precision navigation (time and position), magnetic field, electric field, and electromagnetic field sensing, and development of noisy intermediate- and large-scale quantum processors that can be heavily exercised to find what problems they can tackle that are difficult or impossible for classical processors."[36] However, doing so requires more than simply investing in specific areas of QIS. To ensure that the U.S. military is able to realize the full benefits of this emerging field, it will be important to foster partnerships between industry and academia to guarantee a competent workforce and avoid a talent shortfall.[37] Finally, there are numerous commercial applications that themselves could serve to strengthen the U.S. economic and defense industrial base.

The larger trendline, however, is unmistakable. The continued development of quantum computing is critical for the future of U.S. security.[38] Policymakers in Washington would do well to continue funding plans for quantum technologies. They would also be prudent to keep a watchful eye on the advances made by America's adversaries, so as to ensure that the U.S. remains on the cutting edge of the quantum revolution.

ENDNOTES

[1] Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature* 574, 505–510, October 23, 2019, https://www.nature.com/articles/s41586-019-1666-5.
[2] John Preskill, "Why I Called It 'Quantum Supremacy,'" *Quanta Magazine*, October 2, 2019, https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/
[3] Arute et al., "Quantum supremacy using a programmable superconducting processor."
[4] Edwin Pednault, John Gunnels, Dimitri Maslov, and Jay Gambetta, "On 'Quantum Supremacy,'" *IBM Research Blog*, October 21, 2019, https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/
[5] Daphne Leprince-Ringuet, "Quantum computers are coming. Get ready for them to change everything," *ZDNet*, November 2, 2020, https://www.zdnet.com/article/quantum-computers-are-coming-get-ready-for-them-to-change-everything/
[6] Timothy M. Persons, "Science and Tech Spotlight: Quantum Technologies," Government Accountability Office, May 2020, https://www.gao.gov/assets/710/707204.pdf
[7] Klon Kitchen, "Quantum Science and National Security: A Primer for Policymakers," Heritage Foundation *Backgrounder* no. 3385, February 5, 2019, https://www.heritage.org/technology/report/quantum-science-and-national-security-primer-policymakers
[8] Persons, "Science and Tech Spotlight: Quantum Technologies."
[9] Patricia Moloney Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations," *Congressional Research Service Report* R45509, November 1, 2019, https://crsreports.congress.gov/product/pdf/R/R45409
[10] Ibid.
[11] Sam Sattel, "The Future of Computing," https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/
[12] Scott Buchholz et al., "The realist's guide to quantum technology and national security," *Deloitte Insights*, February 6, 2020, https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html
[13] U.S. Department of Defense, Defense Science Board, "Applications of Quantum Technologies Executive Summary," October 2019, https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf; Leprince-Ringuet, "Quantum computers are coming. Get ready for them to change everything."
[14] National Security Agency Central Security Service, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," n.d., https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/
[15] Persons, "Science and Tech Spotlight: Quantum Technologies."
[16] U.S. Department of Energy, "U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event," July 23, 2020, https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet

[17] Army Research Laboratory, "Scientists create quantum sensor that covers entire radio frequency spectrum," Phys.org, March 19, 2020, https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html?fbclid=IwAR3p-KVZa3q8Wv37VveeAl1dJrO70I9aPDloxNqwYxdhN-eQjYu3WfRqSgMEA
[18] Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations."
[19] Defense Science Board, "Applications of Quantum Technologies Executive Summary."
[20] Persons, "Science and Tech Spotlight: Quantum Technologies."
[21] Elsa B. Kania and John K. Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," Center for a New American Security, September 2018, https://www.cnas.org/publications/reports/quantum-hegemony
[22] Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations."
[23] Ibid.
[24] Tom Stefanick, "The State of U.S.-China quantum data security competition," Brookings Institution *Tech Stream*, September 18, 2020, https://www.brookings.edu/techstream/the-state-of-u-s-china-quantum-data-security-competition/
[25] Kania and Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership."
[26] Persons, "Science and Tech Spotlight: Quantum Technologies."
[27] Ibid.
[28] Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations."
[29] Persons, "Science and Tech Spotlight: Quantum Technologies."
[30] National Science and Technology Council, "National Strategic Overview for Quantum Information Science," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf
[31] Stefanick, "The State of U.S.-China quantum data security competition."
[32] Persons, "Science and Tech Spotlight: Quantum Technologies."
[33] Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations"; Michael Kratsios and Chris Liddell, "The Trump Administration Is Investing $1 Billion in Research Institutes to Advance Industries of the Future," White House Office of Science and Technology Policy, August 26, 2020, https://www.whitehouse.gov/articles/trump-administration-investing-1-billion-research-institutes-advance-industries-future/
[34] Figliola, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations."
[35] Stuart A. Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD," Institute for Defense Analysis, *IDA Document* D-10709, July 2019, https://www.ida.org/-/media/feature/publications/o/ov/overview-of-the-status-of-quantum-science-and-technology-and-recommendations-for-the-dod/d-10709.ashx
[36] Ibid.
[37] Defense Science Board, "Applications of Quantum Technologies Executive Summary."
[38] National Science and Technology Council, "National Strategic Overview for Quantum Information Science."

Electronic Warfare and Cybersecurity Eye the Future

Eric Ormes

The primary tenet of electronic warfare (EW) has remained steadfast since its early conception in the first half of the 20th century, and endures today on the modern battlefields of the 21st. This prime directive can be summed up simply as, "Dominate the electromagnetic (EM) spectrum." While that principle remains unchanged, the means and mechanisms through which the objective is achieved are undergoing nothing short of a revolution. As reliance on digital technologies that enable command and control (C2) continues to expand, the potential attack vectors for these systems bleeds from the physical realm into the cyber domain. This shift, and the resulting entanglement of electronic warfare with cyber warfare, will lead to battlefield evolutions stretching well beyond the next century.

FROM WAVES TO BITS AND BYTES

Italian inventor Guglielmo Marconi's creation, in the late 19th century, of the first practical radio transmitters and receivers ushered in a new era of technological advancement.[1] Though designed originally for commercial purposes, radio—along with other future technologies such as radar—would soon find its footing within military applications.

In every use of these technologies, the physics governing them remains the same: an EM wave is generated by a transmitter, with the objective of being picked up by a receiver. What has changed, though, is how these signals are translated into the data seen, or heard, by the intended receivers. As an example, digital radio processes the received signal into patterns of numbers, whereas analog radios process them into patterns of electrical signals resembling sound waves.[2] The moment that computer processing analyzes and translates the raw signal into an executed action, a new method of conducting electronic warfare is present.

In order to launch an attack against the underlying computer that processes the information, only a pathway to that device is required. In the case of a system such as radar, which relies on receiving a return signal from its originally transmitted one, inherent trust is placed in the return signal. The computer processing the radar system has no reason to believe a return signal would come from anything but a trusted source—its own radar transmitter.[3] As a result, just like with the early internet, where trust and authentication weren't considered primary necessities, cyber attack methods have gained a foothold in this domain.

CYBER ELECTRONIC ATTACK AND AIR DEFENSES

One of the most prolific areas of electronic warfare has been executing electronic attacks against air defense systems. Until the end of the 20th century, most of these attacks traditionally focused on defeating the ability of radars to receive accurate information based on the EM return signals, or to use the radar's EM transmissions to help guide anti-radiation weapons to destroy the target. However, advances by weapons developers that incorporate digital technology into modern advanced air defense systems has resulted in the development of newer tactics utilizing computer network attack-based methods to execute traditional electronic attacks, with devastating results.

One of the first publicly documented cases of this new age cyber electronic attack was witnessed in 2007 during "Operation Orchard," as the Israeli attack against the Al Khibar Syrian nuclear reactor in the Deir ez-Zor region of Syria is known. During this operation, eight non-stealth-capable Israeli aircraft penetrated Syrian airspace, destroying their target and returning to base without alerting the Syrian air defense network.[4] The operation was made possible because the Israeli Air

***Eric Ormes** is a Senior Fellow in Defense Studies at the American Foreign Policy Council, focused on Cybersecurity and Information Technology and Innovation. He is a former United States Air Force officer and is a current cybersecurity practitioner with experience across multiple industries.*

Force, utilizing EW aircraft, took over the Syrian air defense network and fed it a "false-sky picture," leading computers and personnel alike to believe that no threats were in the air at the time of the attack.[5] While the exact details of the incident have not been openly reported, many believe it to have utilized a system similar to BAE's Suter computer program, which is designed to launch computer base attacks against networks and communications systems.[6]

Advances by weapons developers that incorporate digital technology into modern advanced air defense systems has resulted in the development of newer tactics utilizing computer network attack-based methods to execute traditional electronic attacks, with devastating results.

Suter, based on descriptions that have been made public, mirrors the capabilities of many malware families that have targeted businesses and governments around the world for years. The ability to allow attacking operators to perform actions that range from seeing information being fed to end users to escalating privileges to the administrator level are all common tactics, techniques, and procedures (TTPs) seen in everyday cyber attacks. The only difference is how the malicious payload gets to the target system. The options come down to two main choices; either attackers already have a pathway (wired or wireless) on the network connected to the air defense system, or malware, under the guise of a return signal, is beamed to the radar receiver. The host computer, without reason (or potentially even the ability) to authenticate that this signal is trusted or valid, will begin to read and process the received signal. Except in this case, the signal is specially crafted to exploit some underlying vulnerability within the radar's processing unit, allowing the attackers to perform any number of scenarios, from feeding false information to pointing the radar away from attacking aircraft to even potentially shutting down the whole system.

Currently, "Operation Orchard" remains the one prominent public instance where probable cyber attack TTPs have been used as part of a direct military action in the EW domain. Yet the evolution of EW platforms to include cyber components suggests that similar instances are likely to emerge in the future.[7]

ELECTRONIC WARFARE, DRONES, AND CODE

A newer dynamic in EW is the increased use of drones to execute military operations in place of traditionally manned assets. The reliance on the EM spectrum for these devices to be remotely controlled, send vital telemetry, or receive in-mission updates means that they face a greater risk from electronic warfare than do most manned devices. The importance of their connection to the EM spectrum cannot be understated; it is, quite simply, the core of their functionality. Yet even before these systems make it to the field, the code that is pushed out to them—either from a fresh installation or an in-the-field update—provides another point of entry for attackers.

In December 2011, Iranian state media showed the world what appeared to be a relatively intact, captured U.S. RQ-170 drone. Though Iranian authorities claimed to have shot down the drone, there appeared to be very little damage to the aircraft, suggesting that hostile fire wasn't the cause of the downing. This, in turn, led to various theories regarding how the drone was actually acquired by the Iranians, ranging from it being hacked, having its systems jammed, or that the drone itself had executed pre-programmed protocols based on a specific scenario.[8]

In the end, the most plausible explanation appears to be that a combination of techniques related to EW and cyber TTPs may have been used to bring down the drone. Based on the account of an Iranian engineer

who claimed to have worked on reverse engineering the drone technology, the craft was brought down by jamming the RQ-170's communication link and then exploiting a vulnerability in its GPS system. Simply put, the Iranian side tricked the drone into thinking it had returned to its home base in Afghanistan, and got it to land on Iranian territory instead.[9]

Regardless of how the RQ-170 was brought down, the specter of potential vulnerabilities in the computer and communications systems of drones has pushed industry to work to protect against similar situations in the future.[10] To help reduce the risk posed by the reliance on external connections to various networks for remotely operated drones, manufacturers will have to increase the sophistication of their on-board software. In turn, as drones become more self-contained and isolated to shield them from external attack vectors, reliance on their on-board logic increases. This, in turn, creates another vulnerability: an opportunity for adversaries to focus on the "Achilles Heel" of all computer systems, namely the source code that runs and operates all modern programs and applications.

A newer dynamic in EW is the increased use of drones to execute military operations in place of traditionally manned assets. The reliance on the EM spectrum for these devices to be remotely controlled, send vital telemetry, or receive in-mission updates means that they face a greater risk from electronic warfare than do most manned devices.

ROOT PROBLEMS

In May of 2017, a cybersecurity researcher discovered an unsecure Amazon Simple Storage Service (S3) bucket had been publicly exposed on the internet by a defense contractor with files connected to the U.S. National Geospatial-Intelligence Agency (NGA), which provides battlefield satellite and drone surveillance imagery for the U.S. military. Within the S3 bucket was information that could have given attackers access to where source code was stored.[11] In an EW scenario, analyzing this code could lead adversaries to develop their own Suter-like attack against a class of assets by beaming seemingly benign signals that exploit the underlying software.

Furthermore, the FBI reported in early November 2020 that, for at least the previous seven months, threat actors had been exploiting misconfigured instances of the application security tool SonarQube.[12] This tool, used to check source code for vulnerabilities, was being exploited by malicious actors to instead steal source code, victimizing multiple U.S. government agencies and private businesses in the process. Again, stealing this code allows adversaries to gain in-depth knowledge about how these programs function, as well as potential insights into the hardware they are supporting. In the case of code used in battlefield systems, such an exploitation could give adversaries key tactical knowledge and allow them to develop appropriate EW or cyber countermeasures.

Besides getting critical intelligence about systems by stealing their source code, attackers can also attempt to "poison the well" by introducing malicious elements into the code. In May of 2020, Github (a company that specializes in maintaining code repositories for customers) issued a security alert about malware they had seen that was capable, among other things, of altering source code with malicious elements. A change of this type, if left undetected, could allow attackers to successfully disrupt, *en masse*, every system that receives the poisoned version of code. An example of this technique's devastating effect was recently seen with the December 2020 SolarWinds cyber attack, where a seemingly authentic update

to SolarWinds software was in fact poisoned by malicious actors to deliver malware to potentially thousands of victims. While remote, isolated drones will rely heavily on code, even manned systems would be susceptible to poisoned software. An adversary that wishes to disrupt air defense systems, communications networks, or weapons systems that rely upon the EM spectrum no longer need sophisticated EW methods to achieve these objectives; just a few well-placed lines of code will do.

THE END…?

So where does that leave the future of electronic warfare, and cyberwarfare's role within it? While some say the two fields are distinct and separate, we now see them becoming more and more intertwined. As more technologies and protocols are taken from the commercial world and integrated into military systems, the ability for cyber attacks to affect them will continue to expand. Conversely, as greater numbers of military systems rely upon the EM spectrum to connect to battlefield networks to receive critical communications and updates through software, the ability to disrupt them through EW will increase. While the methods of attack may differ between the two, they are connected in that they still support the same overall objective, to "Dominate the electromagnetic spectrum."

ENDNOTES

[1] Encyclopedia Britannica, "Gugliemo Marconi," n.d., https://www.britannica.com/biography/Guglielmo-Marconi.
[2] Federal Communications Commission, "Digital Radio," n.d., https://www.fcc.gov/consumers/guides/digital-radio.
[3] Chris Woodford, "Radar," *ExplainThatStuff!*, December 13, 2020, https://www.explainthatstuff.com/radar.html.
[4] David Makovsky, "The Silent Strike: how Israel bombed a Syrian nuclear installation and kept it secret," *New Yorker*, September 17, 2012, https://www.newyorker.com/magazine/2012/09/17/the-silent-strike.
[5] Judah Ari Gross, "Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor," *Times of Israel*, March 21, 2018, https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/.
[6] John Leyden, "Israel suspected of 'hacking' Syrian air defences," *The Register*, October 4, 2007, https://www.theregister.com/2007/10/04/radar_hack_raid/.
[7] J.R. Wilson, "Enabling technologies for airborne electronic warfare," *Military & Aerospace Electronics*, February 28, 2020, https://www.militaryaerospace.com/sensors/article/14168864/airborne-electronic-warfare.
[8] Scott Peterson, "Downed US drone: How Iran caught the 'beast,'" *Christian Science Monitor*, December 9, 2011, https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.
[9] Scott Peterson and Payam Faramarzi, "Exclusive: Iran hijacked US drone, says Iranian engineer," *Christian Science Monitor*, December 15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.
[10] John Keller, "Iran-U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking," *Military & Aerospace Electronics*, May 3, 2016, https://www.militaryaerospace.com/computers/article/16715072/iranus-rq170-incident-has-defense-industry-saying-never-again-to-unmanned-vehicle-hacking.
[11] Sean Gallagher, "Defense contractor stored intelligence data in Amazon cloud unprotected [Updated]," *Ars Technica*, May 31, 2017, https://arstechnica.com/information-technology/2017/05/defense-contractor-stored-intelligence-data-in-amazon-cloud-unprotected/.
[12] Catalin Cimpanu, "FBI: Hackers stole source code from US government agencies and private companies," *ZDNet*, November 7, 2020, https://www.zdnet.com/article/fbi-hackers-stole-source-code-from-us-government-agencies-and-private-companies.
[13] Catalin Cimpanu, "GitHub warns Java developers of new malware poisoning NetBeans projects," *ZDNet*, May 29, 2020, https://www.zdnet.com/article/github-warns-java-developers-of-new-malware-poisoning-netbeans-projects/.
[14] Laura Hautala, "SolarWinds hack continues to spread: What you need to know," *Cnet*, December 24, 2020, https://www.cnet.com/news/solarwinds-hack-hits-major-tech-companies-and-hospital-system-what-you-need-to-know/.

Building Trust in Artificial Intelligence

Neil Serebryany and Mackenzie Mandile

On the evening of June 19, 1815, after a united British-Prussian force defeated Napoleon's army at Waterloo, a carrier pigeon belonging to the House of Rothschild is said to have crossed the English Channel, delivering news of the French Empire's defeat to London a full twenty-four hours before it was officially circulated. Nathan Rothschild was subsequently presented with an opportunity to leverage this information and purchase British government bonds before the market soared the following day.[1]

While many specifics of the tale have been lost to history, Rothschild's actions exemplify how utilizing one's trusted tools can secure a favorable decision advantage. A trained carrier pigeon, in this case, demonstrates how appropriately placed trust in a well-trained asset can afford its owner the intelligence to better understand, analyze, and take action on a given issue.

Similarly, tomorrow's warfighters will place their trust in autonomous and semi-autonomous assets that rely on increasing volumes and velocity of data to achieve and sustain battlefield superiority. Throughout history, technological innovation has enabled militaries to outmaneuver their adversaries. From the Union's masterful use of the telegraph to communicate in real-time throughout major Civil War battles; to Alan Turing's Enigma code-breaking machine in World War II; to the modern encryption systems in quantum cryptography, each advancement enabled an advantage in a battlespace of its time. The changing character of war presents new tools, as well as challenges, amid a shifting strategic landscape. Today, artificial Intelligence (AI) and machine learning (ML) solutions are transforming military decision-making and providing alternatives and insights not previously available.

AI and ML ingest and analyze massive amounts of data to reveal patterns and insights undetectable to humans. However, these insights are not deterministic, so how can we be sure our trust is well-placed? Every aspect of our national security apparatus, from strategy to doctrine down to soldier training, is based on years of experience and learning, with high confidence in the expected results. Building an equivalent trust in AI/ML will require the Department of Defense (DoD) to develop and adopt new standards, tools, and capabilities for testing and validating AI models so their contribution to security, transparency, and reliability can be maximized.

LEADERSHIP IN DEFENSE INNOVATION AND TECHNOLOGY

Since the 19th century, the United States has led the world in technological innovation. In the early 1860s, over 15,000 miles of telegraph cables were laid by the United States Military Telegraph Service, blanketing the East Coast and enabling almost-constant communication between Union generals. The results were transformative; William Sherman recalled a "perfect concert of action" between his forces in Georgia and Ulysses S. Grant's forces in Virginia throughout the autumn of 1864.[2] For the first time in history, senior military officials were able to strategically communicate over long distances, instantaneously directing real-time battles and ensuring victories from hundreds of miles away. A century later, at the height of the Cold War, engineers at the newly minted Advanced Research Projects Agency (ARPA) began a project to link computers at Pentagon-funded research institutions to effectively track and detect over 400 aircraft, continually differentiating friendly aircraft from adversarial ones.[3]

Neil Serebryany *is the Founder and CEO of CalypsoAI, a software company and thought leader in model risk management, T&E, monitoring, and security solutions for AI systems. He holds multiple patents in the field of AI Security, and has appeared in* Inc Magazine, Business Insider, Inside Defense *and* Axios, *amongst others.* ***Mackenzie Mandile*** *is a Content Strategist for CalypsoAI. She previously served as a federal civilian at the Naval Undersea Warfare Center. Her commentary has appeared in* DefenseOne.

As we enter 2021, however, near-peer competitors, most notably China, are outpacing the United States with their growing R&D budgets, their willingness to data-mine their citizens to create massive datasets, and their advancement of robust AI models. Domestically, meanwhile, the U.S. government trails private industry and academia significantly in the leadership of AI innovation. For the first time in history, the United States government is not a technological leader, and must leverage the talent and innovation of private industry.

As we enter 2021, near-peer competitors, most notably China, are outpacing the United States with their growing R&D budgets, their willingness to data-mine their citizens to create massive datasets, and their advancement of robust AI models...For the first time in history, the United States government is not a technological leader, and must leverage the talent and innovation of private industry.

TRUST THROUGH PARTNERSHIP

In the past, the U.S. government and the private sector formed partnerships to leverage innovative, emerging technologies to improve national security. Pre-1990, the art and science of encoding electronic communications known as modern cryptography primarily belonged to the U.S. government. In 1991, however, the development of the world wide web infrastructure merged hypertext with information retrieval, enabling the American public to utilize the internet as an easy yet powerful global information system. Suddenly, the success of the Information Age hinged upon the ability to protect the data flow generated by a rush of e-commerce.

Importantly, throughout the 20th century, only national security agencies and the military possessed computers powerful enough to deploy strong cryptosystems to secure their data transmissions.[4] Through a partnership between IBM, who developed an encryption standard based on the famed Lucifer cipher, and the NSA, who modified IBM's encryption algorithm, the U.S. Data Encryption Standard was born. Private industry successfully leveraged a modified version of the government's powerful tool, allowing the American public to safely conduct business online. The collaborative effort by the government and private sector enabled a far more robust and secure online environment—one that has enabled over three decades of U.S. leadership in the cyber domain.

The current state of AI mirrors that of encryption years ago, where the United States has a window of opportunity to become the global technological leader. However, in order to achieve this objective, the U.S. government must utilize partnership with industry to effectively employ AI as a secure and viable tool.

As with the internet, AI will continue to increase in complexity as research and competition in the field proliferates. Perhaps the most significant challenge in using autonomy for national security is that AI is often insecure. In machine learning, models learn from data, and do not follow a set of programmed rules, effectively teaching themselves how to solve problems. As a result, AI is capable of developing new and innovative strategies to solve problems better and faster than traditional methods. However, these models are often insecure, even to the AI engineers that developed them, who frequently don't have a background or specialization in the field of adversarial machine learning, or in ensuring the integrity of AI models.

Take deep neural networks, the architecture behind deep learning models, for example. The network

is composed of an intricate web of interconnected variables that become tuned as the model trains. Mimicking the human brain, each neuron passes on the information it knows to other nodes within the network. With training, the deep neural network grows larger, using trial and error to solve increasingly complex problems. However, even when AI creators have access to the learning model's decision-making parameters, it is impossible to pinpoint exactly which nodes combined to make decisions.

Herein lies the challenge of secure AI: how do you adequately test a system to ensure that it will provide the correct outcome every time? How do your troops in the battlefield gain trust with a system that even the programmers themselves do not understand?

AI is capable of developing new and innovative strategies to solve problems better and faster than traditional methods. However, these models are often insecure, even to the AI engineers that developed them, who frequently don't have a background or specialization in the field of adversarial machine learning, or in ensuring the integrity of AI models.

The challenge of developing secure, national security applications of AI presents the DoD with an opportunity to harness new technology and, perhaps more importantly, to develop the rulebook for testing and evaluating (T&E) AI to ensure that it is trustworthy and secure. The DoD must work to ensure that national security applications of AI are reliable, transparent, and secure—all of which must be achieved through a rigorous T&E framework. As former Under Secretary of Defense for Policy Michele Flournoy, incoming Director of National Intelligence Avril Haines, and Gabrielle Chefitz articulated in a recent white paper, "Far too little attention is placed on the issue of trust, and especially testing, evaluation, verification and validation (TEVV) of these systems. Building a robust testing and evaluation ecosystem is a critical component of harnessing this technology responsibly, reliably, and urgently."[5]

THE MODERN CHALLENGE

Just as the advent of the telegraph enabled Union generals to gain a battlefield advantage during the Civil War, and how private industry utilized the U.S. government's internet security infrastructure, AI/ML represents yet another opportunity for warfighters to leverage the advantage of emerging technology.

The Department of Defense's 2018 *Artificial Intelligence Strategy* defines artificial intelligence as, "the ability of machines to perform tasks that normally require human intelligence."[6] From logistics and preventative maintenance to command and control to lethal autonomous weapons systems, AI can address a myriad of challenges and problem-sets.

The DoD has correctly identified AI as a critical investment in the defense and national security arena. It is primarily coordinating its efforts through the Joint Artificial Intelligence Center (JAIC), while the Army, Navy, Air Force, and Marines have individually stood up specialized AI task forces. In 2018, Congress mandated the establishment of the National Security Commission on AI, and both the Obama and Trump administrations unveiled AI strategies of their own. More recently, the National Artificial Intelligence R&D Strategic Plan outlined high-level federal R&D priorities. In 2020, the Pentagon's AI Ethics Principles further outlined how the Department shall "invest in the research and development of AI systems that are

resilient, robust, reliable, and secure; we will continue to fund research into techniques that produce more secure AI; and we will pioneer approaches for AI test, evaluation, verification, and validation."[7] Yet the DoD has still to translate this goal into actionable strategies.

The success of AI in national security settings hinges on warfighters' ability to trust their autonomous assets. Activating autonomous systems on the battlefield is an act of trust, and delegating tasks to machines inevitably grants those machines more power. For example, military leaders were initially reluctant to deploy drones because they trusted a human pilot's years of training and experience over that of drone technology. AI, similarly, will require warfighters to build trust over time. High-reliability operations of autonomous systems are possible, but they require testing and training in partnership with warfighters.

The success of AI in national security settings hinges on warfighters' ability to trust their autonomous assets. Activating autonomous systems on the battlefield is an act of trust, and delegating tasks to machines inevitably grants those machines more power. For example, military leaders were initially reluctant to deploy drones because they trusted a human pilot's years of training and experience over that of drone technology. AI, similarly, will require warfighters to build trust over time.

Developing defense applications of AI before our adversaries do may not matter if our systems are brittle, untrustworthy, and continue to be characterized as black boxes. To counter these challenges, the DoD must develop a robust and actionable T&E strategy. As discussed in a recent report from the Center for New American Security, "[The United States] is one of the few countries in the world that can rally its resources and its human capital to achieve the most ambitious of goals. The United States stands at the cusp of another such moment. Prudent policy decisions today will help to protect and cement America's lead in AI for decades."[8]

The DoD's leadership must clearly articulate the parameters for "successful" AI applications in national security, and must leverage a robust testing environment to verify the validity and robustness of those systems. Only by enabling a framework through which AI can be trusted will warfighters be able to leverage it as a viable decision-making asset.

A TRUSTED AI FRAMEWORK

The current state of trusted national security applications of AI is characterized by technological challenges and bureaucratic barriers. The United States has a window of opportunity to become the global technological leader in this arena. As it did in the past with the development of standard encryption, the DoD must join forces with industry partners to build AI that is secure and trustworthy. However, for the United States government to effectively leverage the private sector's powerful AI solutions, the DoD must reduce barriers to AI adoption through the development of standards, tools, and new capabilities.

First, the United States government, broadly, must create a rulebook that concisely articulates the standards that all national security applications of AI will be tested against to ensure their efficacy and validity. This framework must incorporate the DoD's existing legal and ethical requirements, and

should provide T&E guidance for DoD Directive 3000.09, which establishes national policy on the development and deployment of lethal autonomous weapons systems. Both the JAIC and NIST will be releasing trusted AI roadmaps in 2021, and those frameworks should incorporate reliability metrics, model performance evaluation, explainability reporting, and evaluations of data sourcing, against which all AI can be measured. Without these key report functions, it is difficult to assess the validity and efficacy of AI/ML systems. As Flournoy, Haines, and Chefitz recommend, "A DoD-wide testing framework for AI/ML will help shorten the testing cycle and make test results interpretable and comparable across the Department." [9] In light of the DoD's intent to utilize AI on the modern battlefield, it is imperative that warfighter trust in these autonomous assets is well-placed.

Second, the current DoD testing environment is not well-suited to address the unique challenges presented by adaptive technologies like AI/ML, and the Department should consider implementing industry best-practices for AI T&E. For decades, the DoD has utilized a set of processes and tools to test and measure hardware-intensive systems before they are fielded. But AI functions in an entirely different way than does a tank, for example, and requires a new testing ecosystem as a result.

In private industry, trustworthy AI is developed by addressing a constellation of risk factors, which are evaluated throughout the life cycle of a model. Utilizing a Secure Machine Learning Lifecycle (SMLC), AI creators and end-users can peer behind the curtain of the most powerful AI. The SMLC ensures that data scientists adhere to best practices throughout AI development, and provides a secure environment for a model to train, protecting it from adversarial attacks. When leveraging an end-to-end T&E framework, developers can manage threats across the algorithm life cycle, calibrate data to ensure only fair metrics influence the model, and conduct tests to identify and address data bias and model drift, among other factors. T&E tools enable the verification and validation of AI efficacy through a battery of traditional and non-traditional tests, such as noise injection and intentional data poisoning. When models are developed within an SMLC testing framework, AI creators and mission owners alike are empowered to make well-informed decisions about how and whether to deploy their AI, or if their model requires additional training.

Developing defense applications of AI before our adversaries do may not matter if our systems are brittle, untrustworthy, and continue to be characterized as black boxes. To counter these challenges, the DoD must develop a robust and actionable testing and evaluating strategy.

Finally, to lower the barriers to AI adoption, the U.S. government must set a benchmark for AI testing infrastructure. Here, the U.S. can look to the global community and implement extant frameworks such as the European Union's white paper on trusted AI[10]; the European Parliament's ethical AI implementation strategy[11]; and the Australian Institute of Standards ethical AI roadmap.[12] Alternatively, it could build one of its own, integrating many of the testing and certification recommendations for AI/ML that are being advocated by our international partners. Whatever path it takes, by developing a testbed that leverages the innovation of American private industry and adopting implementation strategies in line with the global AI community, the U.S. government can enhance AI/ML security and robustness. Further, such a testing framework will provide powerful insight into AI applications and quantify their capabilities, enabling warfighters to utilize trusted AI tools and teammates.

LOOKING AHEAD

Throughout history, the ability to obtain data and conduct insightful analysis has enabled actors to make informed decisions with increasing agility. Exploiting emerging technology is an enduring cornerstone of securing decision advantage. From the telegraph to artificial intelligence, leveraging trusted assets continues to enable policymakers to have a better operating picture.

AI and ML are transformational technologies with applications in nearly every sector of government and private industry. Realizing AI's full potential will challenge how we think about engineering and design. It will require partnerships that combine data scientists, ML developers, robust T&E frameworks, and mission domain experts. Perhaps most fundamentally, it will require us to set a higher standard of honesty and transparency in technology for the global community.

ENDNOTES

[1] "Rothschilds and pigeon post," The Rothschild Archive, n.d, https://www.rothschildarchive.org/contact/faqs/rothschilds_and_pigeon_post.

[2] See, for instance, David Hochfelder, "The Telegraph," Essential Civil War Curriculum, n.d., https://www.essentialcivilwarcurriculum.com/the-telegraph.html.

[3] Defense Advanced Research Projects Agency, DARPA: 1958-2018, 2018, https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf

[4] For an early history, see Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, 2000).

[5] Michele Flournoy, Avril Haines and Gabrielle Chafitz, *Building Trust through Testing: Adapting DOD's Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems* (WestExec Advisors, October 2020), https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf.

[6] Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[7] Ibid.

[8] Martijn Jasser et al., *The American AI Century: A Blueprint for Action*, Center for a New American Security, December 17, 2019, https://www.cnas.org/publications/reports/the-american-ai-century-a-blueprint-for-action.

[9] Flournoy, Haines and Chafitz, *Building Trust through Testing*.

[10] European Commission, *WHITE PAPER: On Artificial Intelligence – A European Approach to excellence and trust*, February 19, 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[11] European parliament, "EU guidelines on ethics in artificial intelligence: context and imple-mentation," n.d., https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

[12] Standards Australia, *An Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard*, n.d., https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/O_1515-An-Artificial-Intelligence-Standards-Roadmap-soft_1.pdf.aspx.

Shaping the Aerial Battlefield of the Future

Cody Retherford

As global focus shifts from counterinsurgency back to conventional state-based conflict, airborne weapon systems are becoming exponentially more important to the prosecution of combat operations. Air superiority was a given during the counterinsurgencies of the last two decades, but will be heavily contested in a modern conventional conflict. The battle for air superiority between major state powers demands increasingly unconventional, innovative thinking—both technologically and tactically—to maintain the edge over adversaries. New technology must be economically viable, secure from cyber and electronic warfare attacks, and adaptable to the rapidly-changing battlefield.

The current aerial arms race focuses on capabilities to support suppression of enemy air defense (SEAD), to win in air-to-air combat, and to engage satellites in space to ensure dominance. Artificial Intelligence (AI)-driven combat aircraft, drone swarms, and laser weapons will become essential force multipliers in the skies above future conflict.

AI COMBAT AIRCRAFT (LOYAL WINGMAN)

The "loyal wingman" concept is being developed due to the extremely high cost of 5th generation and 6th generation manned stealth fighter aircraft, and the extremely high risk to pilots and aircraft in high intensity conventional conflict. Loyal wingman autonomous combat drones provide a cheap force multiplier that can execute Intelligence, Surveillance, and Reconnaissance (ISR), Electronic Warfare (EW), and fire support missions in conjunction with manned aircraft, all with no added risk to human life. In the future, they may replace manned aircraft all together. DARPA is currently testing AI based on human strategic decisions for air-based combat platforms.[1] Furthermore, the U.S. Air Force is testing AI-piloted combat aircraft that regularly defeat actual pilots in simulations.[2] AI-powered drones make decisions more efficiently than do human pilots, and are not susceptible to human limitations such as G-Forces.

United States—The USAF is focusing heavily on the *Skyborg* AI System, which is meant to autonomously fly a variety of mission specific, inexpensive drone systems in support of manned aircraft.[3] Four defense contractors are currently developing AI-enabled drone platforms meant to be operated by Skyborg.[4] The most public example remains the *Kratos* XQ-58A.[5] The USAF is also known to be testing air-launched loyal wingman drones including the *Kratos* UTAP-22.[6] The *Skyborg* system is designed to be adaptable to new platforms.

United Kingdom—The British Royal Air Force (RAF) is pursuing similar low cost AI-driven drone systems to amplify manned combat aircraft capabilities through *Project Mosquito*. Three defense contractors are currently building demonstrators that are meant to work with British F-35s and Typhoons or autonomously in ISR, EW, and direct strike roles.[7] The project aims to lower the costs, risks, and manpower requirements of aerial capabilities while also increasing wide area reconnaissance and explosive ordinance detection capabilities.[8]

Australia—The Royal Australian Air Force (RAAF) is further along than its British counterpart, currently working with Boeing to develop the Airpower Teaming System (ATS), which is similar in concept to the *Kratos* XQ-58A. The ATS integrates a rapidly swappable payload design on one airframe to ensure readiness for air-to-air, ISR, EW, direct strike, and airborne early warning mission sets.[9] The drone will be AI-driven and will operate autonomously, independently or alongside manned aircraft.[10]

Cody Retherford *is a junior fellow at the American Foreign Policy Council. He contributes to the* Iran Democracy Monitor *and the* World Almanac of Islamism*. He is a former US Army officer with experience in light infantry and special operations.*

Russia—The Russian Aerospace Forces (VKS) are testing two potential loyal wingman candidates. The "Kronshtadt Grom" is an autonomous system designed to support manned aircraft and to conduct SEAD strike missions.[11] The *Sukhoi* S-70 "Okhotnik" is similarly designed to autonomously support manned aircraft, but is also designed to conduct Suppression of Enemy Air Defense (SEAD) as well as air-to-air missions.[12] Both airframes are currently being tested in conjunction with 5th generation Russian fighter aircraft.

China—The Peoples' Liberation Army Air Force (PLAAF) maintains a high level of secrecy around their loyal wingman program. Although information is limited, the Chinese are known to be developing the LJ-1 drone system. The drone is similar to other systems aimed at providing autonomous EW and fire support to manned aircraft.[13] The key difference in the Chinese system is that the LJ-1 is designed to act not just as a loyal wingman, but also as a loitering munition or suicide drone as needed.

AI DRONE SWARMS

The drone swarm is a dynamic concept whose applicability ranges from large loyal wingman drones to small loitering munitions covering a myriad of missions, including SEAD, offensive and defensive EW, wide area ISR for manned aircraft and ground-based long range precision fire assets, and direct strike missions. The conflict between Azerbaijan and Armenia over Nagorno-Karabakh shows the importance of cheap, expendable drones used in ISR and direct strike mission sets. While not autonomous systems and largely operated in small numbers on any given mission, the variety and volume of drones deployed by the Azerbaijani military contributed significantly to its success over the Armenian side.[14] That conflict, in turn, points to a future when those drones will be replaced by far more capable AI-driven swarms.

The conflict between Azerbaijan and Armenia over Nagorno-Karabakh shows the importance of cheap, expendable drones used in ISR and direct strike mission sets. While not autonomous systems and largely operated in small numbers on any given mission, the variety and volume of drones deployed by the Azerbaijani military contributed significantly to its success over the Armenian side. That conflict, in turn, points to a future when those drones will be replaced by far more capable AI-driven swarms.

United States—In conjunction with the loyal wingman drone systems, the U.S. is developing a variety of smaller drones for use in swarm-based mission sets. The DARPA Gremlins Drone Swarm Program is testing the *Dynetics* X-61A, an air-launched drone meant to be used in swarms for direct strike and ISR missions.[15] The General Atomics *Sparrowhawk* aims to compete in the same market.[16] The drones are meant to launch from large drone platforms and transport aircraft. Air-launching provides additional range and capability to drone operations in hard to reach and non-permissive environments. Further, the USAF is developing a unique autonomous swarm capability for guided munitions and decoy devices called the "Golden Horde" which could be used directly with the *Skyborg* program.[17] The systems combined will be utilized to both disrupt and destroy air defenses and other ground targets.

United Kingdom—While the UK's *Project Mosquito* programs are meant to be operated

in swarms in the future, the UK is also developing additional drone swarm technology including *BriteCloud*. *BriteCloud* is an expendable swarm of autonomous EW drones focused on jamming air defenses. The system detects radar signals and broadcasts mimicked signals to disrupt radars and surface-to-air missiles.[18]

Russia—The Russians are regularly executing major training exercises utilizing drone swarms. Drone swarms have successfully executed EW missions disrupting enemy air defense systems and conducted direct strikes on C2 nodes and other ground targets.[19] They have also been used extensively to conduct ISR in support of long-range precision fire artillery assets.[20] Russia is rapidly incorporating drone swarm technology and tactics into its military strategy.

China—The Chinese are also testing and training drone swarm technology. The Chinese military recently tested a new launching system that fires a swarm of CH-901 loitering munitions. Those munitions are also capable of being air-launched from fixed wing platforms and utilized to overwhelm air defense sensors and strike ground targets.[21] Chinese technology is increasingly focused on multi-role capabilities as well, including suicide strikes.

LASER WEAPON SYSTEMS

Laser-based weapon systems are the definitive future of aerial warfare, but currently face a critical dilemma over power-to-weight ratio. The stronger the laser, the more power is required to operate it, leading to larger batteries and increased weights. The country that successfully launches a viable airborne laser weapon system first will gain critical strategic advantages, with the system having potential to be used for direct air-to-air combat, SEAD, and potentially anti-satellite operations. Laser weapon systems are not dependent on locking on radar or heat signatures. Pilots could, in theory, directly target whatever they can see, and engage instantaneously—providing massive advantage over aircraft without similar systems. This will in turn force development of new defensive measures. While incredibly expensive now, advances in technology will cut costs and push laser weapon systems onto the battlefield.

United States—The United States is progressing toward arming fighter and ground attack aircraft with offensive and defensive laser systems. The United States Special Operations Command (USSOCOM) is focused on arming AC-130 gunships with laser weapons as a means of stealthily destroying ground targets.[22] The USAF is aiming to arm fighter aircraft with defensive and eventually offensive laser weapon systems that are meant to replace traditional guns and short-range missiles as a way of advancing air-to-air combat capabilities.[23]

Russia—Known Russian laser weapon systems are focused on airborne and space-based assets. Russia developed an airborne laser system specifically for targeting satellites and airborne ISR sensors.[24] They are also known to have developed anti-missile laser systems for their airborne platforms.[25]

China—The Chinese are also rapidly developing airborne laser weapon systems. The PLA is soliciting bids to develop weapon systems for use both offensively and defensively in air combat, as well as for shooting down missiles.[26] The limited information available regarding these systems indicates that the laser weapons will come in pod form, indicating their applicability for use on both fighters and transport aircraft.[27]

A NEW ARMS RACE

The developments above reflect a stark reality: the state with the most advanced technology and tactics can dominate the skies, and in turn will be able to dominate the battlefield below. Developing innovative technology and tactics with which to employ these systems will become increasingly critical, as global powers return their focus to conventional conflict with peer and near-peer adversaries. In turn, the aerial battles of the future will be controlled from around the world, instead of from the cockpit, as autonomous drone systems become the norm in order to reduce costs and the risk to human life.

ENDNOTES

[1] Brad Bergan, "AI Robot Swarm Learns Tactical Warfare from Video Games," *Interesting Engineering*, February 12, 2020, https://interestingengineering.com/ai-robot-swarm-learns-tactical-warfare-from-video-games

[2] Brian Everstine, "Artificial Intelligence Easily Beats Human Fighter Pilot in DARPA Trial," *Air Force Magazine*, August 20, 2020, https://www.airforcemag.com/artificial-intelligence-easily-beats-human-fighter-pilot-in-darpa-trial/

[3] Joseph Trevithick, "The Fight for the Air Force's 'Skyborg' Artificial Intelligence Equipped Drones has Begun," *The Drive*, May 29, 2020, https://www.thedrive.com/the-war-zone/33567/the-

fight-for-the-air-forces-skyborg-artificial-intelligence-equipped-drones-has-begun

[4] Valerie Insinna, "Four Companies Win Contracts to Build the Air Force's Skyborg Drone," *Defense News*, July 23, 2020, https://www.defensenews.com/unmanned/2020/07/23/four-companies-got-contracts-to-build-the-air-forces-skyborg-drone/

[5] Tyler Rogoway, "Air Force's Secretive XQ-58A Valkyrie Experimental Combat Drone Emerges After First Flight," *The Drive*, March 6, 2019, https://www.thedrive.com/the-war-zone/26825/air-forces-secretive-xq-58a-valkyrie-experimental-combat-drone-emerges-after-first-flight

[6] "Tactical UAVs," Kratos Defense & Security Solutions, n.d., https://www.kratosdefense.com/systems-and-platforms/unmanned-systems/aerial/tactical-uavs

[7] Joseph Trevithick, "Here's Whose in the Running to Build the Royal Airforce's First Loyal Wingman Drones," *The Drive*, June 30, 2020, https://www.thedrive.com/the-war-zone/34498/united-kingdom-will-decide-soon-who-will-build-its-first-loyal-wingman-drones

[8] George Allison, "Royal Air Force Swarming Drone Project 'Exceeding Expectations,'" *UK Defence Journal*, June 22, 2020, https://ukdefencejournal.org.uk/royal-air-force-swarming-drone-project-exceeding-expectations/

[9] Tyler Rogoway, "Everything We Learned from Boeing about its Potentially Game Changing Loyal Wingman Drone," *The Drive*, May 4, 2020, https://www.thedrive.com/the-war-zone/33271/everything-we-learned-from-boeing-about-its-potentially-game-changing-loyal-wingman-drone

[10] "Airpower Teaming System," Boeing, n.d., https://www.boeing.com/defense/airpower-teaming-system/

[11] Aishwarya Rakesh, "Russia's New Stealth Drone, Su-57 Jet Team to Destroy Adversary's Air Defense," *Defense World*, August 25, 2020, https://www.defenseworld.net/news/27712/Russia___s_New_Stealth_Drone_May_Destroy_Adversary___s_Air_Defenses#.X7hKf2hKguU

[12] Kyle Mizokami, "Russia's 'Hunter' is Unlike Anything in America's Arsenal," *Popular Mechanics*, August 10, 2020, https://www.popularmechanics.com/military/aviation/a33548209/russia-hunter-combat-drone/

[13] Kyle Mizokami, "China's Loyal Wingman Drone Flies Alongside Manned Fighters," *Popular Mechanics*, August 23, 2020, https://www.popularmechanics.com/military/aviation/a28845055/china-loyal-wingman-drone/

[14] David Hambling, " The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia," *Forbes*, November 10, 2020, https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/?sh=11b4215e5e57

[15] Rachel Cohen, "DARPA's Gremlins Program Accomplishes First Flight," *Air Force Magazine*, January 21, 2020, https://www.airforcemag.com/darpas-gremlins-program-accomplishes-first-flight/

[16] Joseph Trevithick, "General Atomics' Sparrow Hawk Drone-Launched Drone Breaks Cover," *The Drive*, September 25, 2020, https://www.thedrive.com/the-war-zone/36747/general-atomics-sparrowhawk-drone-launched-drone-breaks-cover

[17] Joseph Trevithick, "USAF Wants to Network its Precision Munitions Together into a 'Golden Horde' Swarm," *The Drive*, June 26, 2019, https://www.thedrive.com/the-war-zone/28706/usaf-wants-to-network-its-precision-munitions-together-into-a-golden-horde-swarm

[18] Joseph Trevithick, "RAF Tests Swarm Loaded with BriteCloud Electronic Warfare Decoys to Overwhelm Air Defenses," *The Drive*, October 8, 2020, https://www.thedrive.com/the-war-zone/36950/raf-tests-swarm-loaded-with-britecloud-electronic-warfare-decoys-to-overwhelm-air-defenses?fbclid=IwAR3uy4n0skTppnnxMs_33zn2v2NF7t-xFV0mMORW8DK8mFilAMcLJM6eehY

[19] Joseph Trevinick, "Russian Drone 'Strike Groups' Jammed and Bombed Air Defenses During Huge Exercise," *The Drive*, November 19, 2020, https://www.thedrive.com/the-war-zone/30912/russian-drone-strike-groups-jammed-and-bombed-air-defenses-during-huge-exercise

[20] David Hambling, "Russia Uses 'Swarm of Drones' In Military Exercise for the First Time," *Forbes*, September 24, 2020, https://www.forbes.com/sites/davidhambling/2020/09/24/russia-uses-swarm-of-drones-in-military-exercise-for-the-first-time/?sh=1271bbdf4771

[21] Joseph Trevinick, "China Conducts Massive Test of Suicide Drone Swarm Launched from a Box on a Truck," *The Drive*, October 14, 2020, https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck

[22] Nathan Strout, "Airborne Laser Weapon on Track for 2022 Demonstration," *C4ISRNet*, June 9, 2020, https://www.c4isrnet.com/battlefield-tech/2020/06/09/airborne-laser-weapon-on-track-for-2022-demonstration/

[23] Garrett Reim, "Lockheed Martin aims to put Lasers Weapon on Aircraft in Five Years," *Flight Global*, September 16, 2020, https://www.flightglobal.com/fixed-wing/lockheed-martin-aims-to-put-laser-weapon-on-aircraft-in-five-years/140204.article

[24] "Russia's Almaz Launches Airborne Anti-Surveillance Laser Project," *Defense World*, June 26, 2019, https://www.defenseworld.net/news/25031/Russia___s_Almaz_Launches_Airborne_Anti_surveillance_Laser_Project

[25] Arun Mathew, "Russia Completes Development of Airborne Anti-Satelite Laser Weapon," *Defense Post*, February 26, 2018, https://defpost.com/russia-completes-development-airborne-anti-satellite-laser-weapon/

[26] Minnie Chan, "China's Military is Hinting at Plans for Airborne Laser Attack Weapon," *Business Insider*, January 8, 2020, https://www.businessinsider.com/china-military-hints-at-plans-for-airborne-laser-attack-weapon-2020-1

[27] Kyle Mizokami, "China's Airborne Laser Weapon Would Change Dogfighting Forever," *Popular Mechanics*, January 13, 2020, https://www.popularmechanics.com/military/aviation/a30502725/china-airborne-laser/#:~:text=China's%20Airborne%20Laser%20Weapon%20Would%20Change%20Dogfighting%20Forever,-Jan%2013%2C%202020&text=The%20Chinese%20military%20put%20out,dogfighting%20as%20we%20know%20it.

Reviving the Military Applications of Nuclear Energy

William Schneider, Jr.

There is today a growing consensus among western democratic countries regarding the People's Republic of China (PRC): that the PRC's threats to national sovereignty, economic prosperity, and national security, its blatant violations of human rights, and its disdain for international law represent a threat to the free world.

Military applications have been at the forefront of nuclear energy research for more than 80 years. Its weapons applications (and the adaptation of nuclear energy to provide propulsion for submarines and surface naval combatants) are well known. Yet more than seven decades of experience with nuclear weapons has inverted expectations about their inevitable role in future conflict. Their availability, and lethality, has produced the longest period of time free of warfare between major nations since the 1648 Peace of Westphalia.

However, while the civil applications of atomic energy in electric power generation, medicine, and space exploration are extensive, there has been very little research into its utility for the production of electric power in the defense sector. That represents a significant oversight, because in the United States the defense sector relies on the civil sector for electrical energy and most of its basing abroad. This state of affairs, in turn, creates challenges when U.S. forces are operationally or tactically deployed, and are compelled to use transportable sources of electric power.

EARLY ATTENTION

The early post-World War II period saw interest in the non-weapons application of nuclear power for use in remote sites. The U.S. Army maintained a nuclear electric power program from 1954 to 1977, operating five portable and three fixed nuclear power sites producing 1-10 megawatts of electric power (MWe). However, the systems were complex to operate, and when all costs were considered proved to be more expensive than conventionally fueled alternatives for the environments in which they were operating. Consequently, the Small Reactor program was abandoned.

Figure 1: Army Small Reactor Program[1]

Plant[(a)]	Operation Location	Net Power, megawatt (electrical)	Activation Date	Deactivation Date
PM-1	Sundance, WY[(b)]	1.0	1962	1968
PM-2A	Camp Century, Greenland	1.6	1961	1964
PM-3A	McMurdo Base, Antarctica	1.5	1962	1972
ML-1	Developmental Testing	0.3	1962	1966
MH-1A	Panama Canal Zone	10	1965	1977
(a) All reactors except MH-1A used highly enriched uranium				
(b) PM-1 pressure vessel was entombed on site and is managed under an Air Force Safety Center Permit				

Dr. William Schneider, Jr. *is a member of the AFPC Advisory Board, as well as a Senior Fellow at the Hudson Institute and a Member of the Pentagon's Defense Science Board (DSB). He previously served as Under Secretary of State and Chairman of the DSB.*

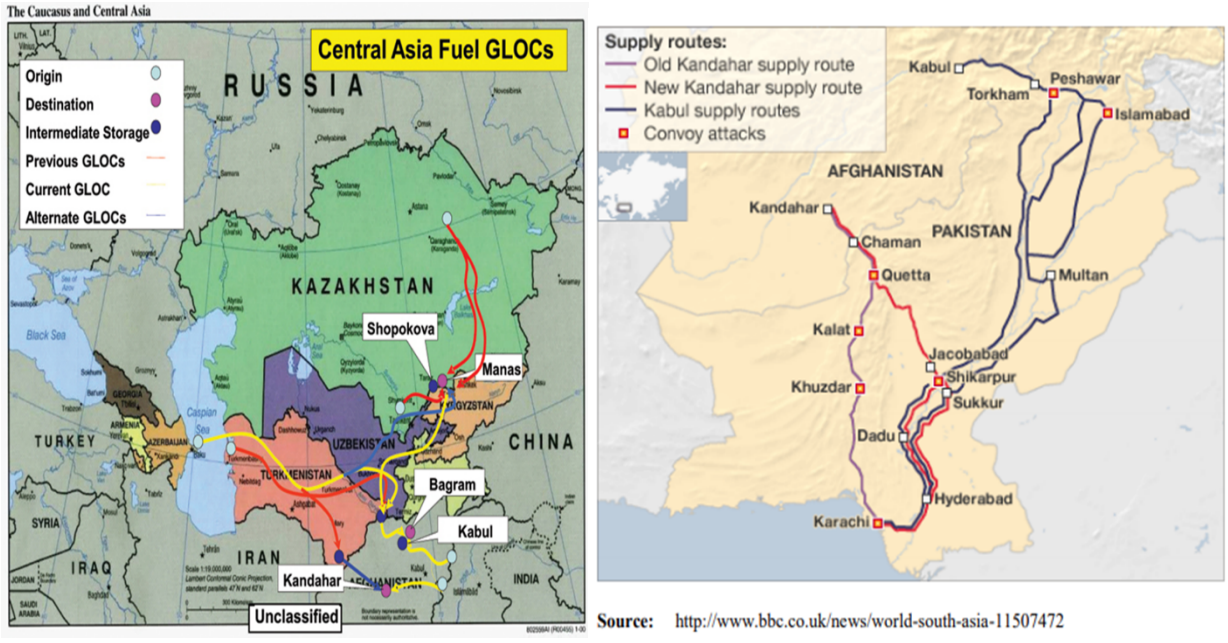
The DoD's electric power epiphany arrived much more recently, as it struggled to provide fuel to support U.S. and allied military operations in Afghanistan and Iraq. The twenty-country region covered by the United States Central Command (USCENTCOM) received more than 5 million gallons of fuel per day, delivered via a Byzantine transportation network of 2,000 commercial fuel trucks supported by 200 million gallons of petroleum storage (see the maps of the Northern and Southern Delivery Networks, below). This fragile logistics system was an attractive adversary target and was treated as such, resulting in significant loss of life.

Secretary of Defense Jim Mattis summarized his own experience with the fuel supply system during his service in Iraq, dubbing it essential to "relieve the dependence of deployed forces on vulnerable fuel supply chains."[2] In doing so, Secretary Mattis repeated the experience of General George Patton 70 years earlier, when Patton's rapidly moving 3rd Army ran out of fuel just outside of Metz, France on August 31, 1944. The epic struggle of U.S. forces to build the Assam-Burma-China pipeline along the "Burma Road" in World War II—the lifeline to allied forces in China—similarly underscored the central role of fuel, and the difficulty of providing it in a contested environment.

The energy-deprived main and forward operating bases (FOBs) from which U.S. tactical ground and air forces operated at the distant end of the tenuous supply line led the DoD to look for alternative approaches. In the future, the DoD will need to mitigate the risk of severed supply lines to the most exposed sites in the current theater of operations.

Over the past two decades, the Defense Science Board (DSB) was tasked by the Secretary to conduct two studies on energy strategy and applications to expeditionary campaigns. The first one, conducted in 2008, was entitled *Task Force On Energy Strategy: "More Fight-Less Fuel."* The second, in 2016, was the *Task*

Figure 2: Fuel Ground Lines of Communication to Afghanistan[3]



Source: http://www.bbc.co.uk/news/world-south-asia-11507472

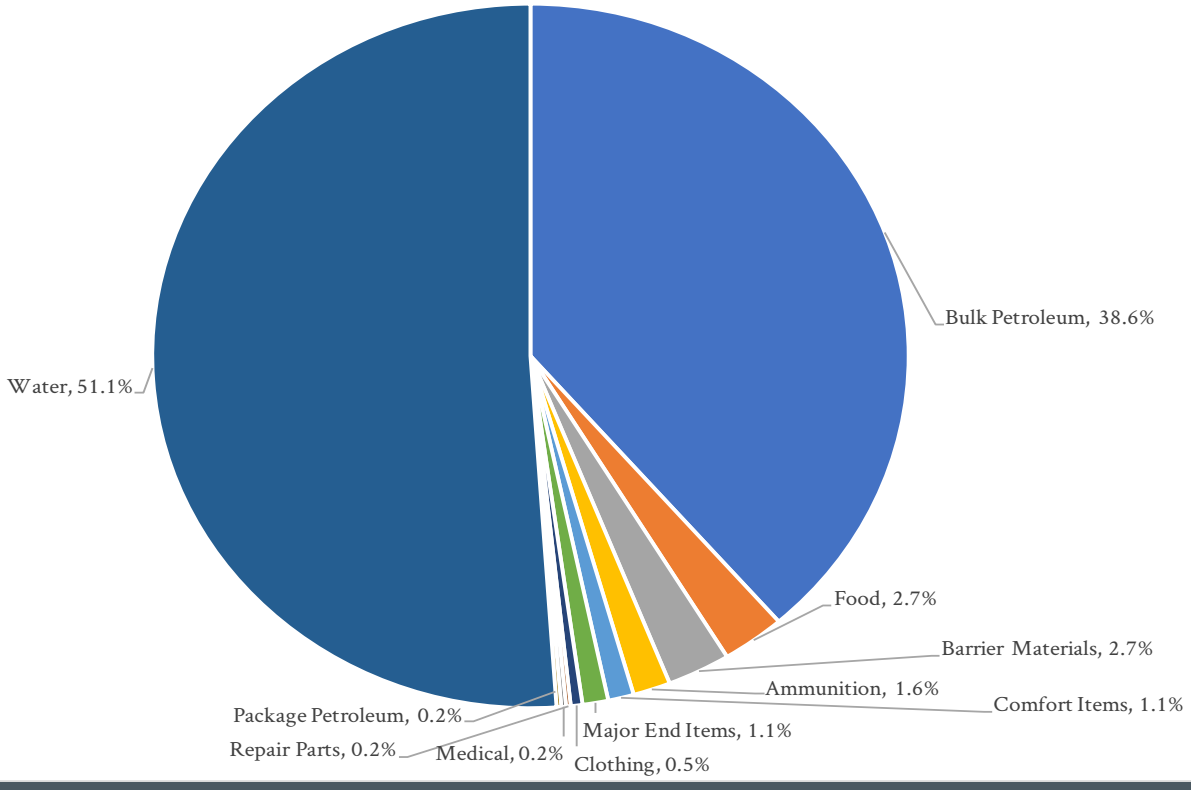
Force on Energy Systems for Forward/Remote Operating Bases. The latter, in particular, served as the stimulus for the DoD's now-funded Project Pele to develop microreactors capable of producing up to 10 MWe for military applications safely and without creating a significant nuclear proliferation risk.

THE PENTAGON'S PROBLEMS

Nearly 90% of the supplies needed for DoD operations are bulk petroleum and water for both remote operating and forward operating bases, as well as main operating bases. In the past, before precision munitions became the mainstay of military operations, ammunition consumption and resupply were a logistical burden on the U.S. supply system. In China's final offensive of the Korean War in July 1953, for instance, 705,000 rounds were fired at U.S. 8th Army and allied forces. The U.S. Army returned the favor, firing 4,711,120 rounds. With non-precision munitions, a U.S. division in a firefight frequently consumed 15,000 tons of ammunition per day in the Korean War.[4] Today, by contrast, the issue is no longer the burden of ammunition delivery; it is the delivery of water and low-energy density fuel for tactical and operational support that has created a significant operational liability for modern military forces.

The support of U.S. and allied operations in Afghanistan has proven to be particularly stressful because of that country's land-locked character. Liquids (water and fuel) need to be brought in by terrestrial convoys involving 350 vehicles per day—75% of the supplies for U.S. and NATO forces—through Pakistan (via the Southern Distribution Network) into Afghanistan. The remainder came from land and air bases in Central Asia (the Northern Distribution Network). These transit corridors were subject to interdiction by adversary elements; 52 percent of coalition casualties in Afghanistan and Iraq between October 2001 and December 2010 were due to attacks

Figure 3: Supply Distribution to Coalition Forces in Afghanistan 2001-10[5]



on overland resupply operations.[6] In a single day in 2008 alone, 96 vehicles were attacked and destroyed in Peshawar, Pakistan *en route* to Afghanistan through the Khyber Pass.

Afghanistan was *sui generis* in the logistics of modern warfare because its land-locked character prevented the seaborne delivery of bulk commodities to the theater. However, 17 countries in Africa also have no access to the sea, while other features such as well-placed seaports and access to them could emerge as significant factors as well. The rise of adversary cyber and other "left-of-launch" capabilities have also exposed a new vulnerability that undermines more than two centuries of the homeland as a military and industrial sanctuary. Since all operating bases in the U.S. use the civil electric power infrastructure for their supplies, disruption of these facilities could diminish or even prevent the U.S. from being able to deploy its forces abroad in a crisis.

The DoD is currently spending some $1.6 billion annually on the development of renewable energy technologies that can mitigate military dependence on conventional fuels.[7] There are likely to be many opportunities within the scope of DoD operations where energy density and storage technology will meet mission requirements. However, the DoD's emerging capabilities are energy intensive and will require a transition to significantly higher energy-density fuels. For example, high energy lasers and microwave weapons, railguns, and related capabilities require high energy density sources.

Fortunately, the past decade has seen the evolution of technology that may permit the revival of an abandoned energy source: nuclear power. The mention of nuclear power conjures images of fragile gigawatt scale plants that are vulnerable to a multitude of miscues. However, new technology can mitigate or eliminate the risks associated with nuclear energy, and in so doing may promote a paradigm shift in military operations by converting the energy-deprived forward and remote operating bases into energy abundant sites that can impart significant tactical and operational advantages.

RELEVANT TECHNOLOGY

The energy density of Uranium 235 is extraordinary; two million times greater than diesel fuel. That makes it a compelling choice for addressing the core DoD requirement of ensuring the resiliency of forward and remote operating bases against potential disruption of energy supplies. That is a real danger today; most bases use less than 10 MWe to meet day-to-day needs, but have less than five days of fuel supplies in reserve.

Figure 4: Fuel Energy Density[8]

Fuel Type	Energy Density (kJ/kg)
Gasoline	44,000
Kerosene	43,300
Diesel	43,200
Uranium 235	67,300,000

Nuclear energy offers a path to converting energy-deprived main operating and forward bases into energy-abundant ones, with profound implications for the conduct of military operations. Instead of needing to rely on transported water and fuel for its vehicles and aircraft, abundant electrical power will enable the installation to produce its own.

Moreover, changing technology will permit the new nuclear power system to be air-transportable (in a C-17-class aircraft) or road/rail transportable in a standard 40-ft. shipping container. The existence of energy abundance at forward sites, in turn, could facilitate the employment of energy intensive weapon systems such as high energy lasers, electromagnetic rail guns, non-nuclear electromagnetic pulse weapons, and others. Back in the 1950s, Los Alamos National Laboratory (LANL) developed very small ("waste basket" size) microreactors of an entirely new design concept for the National Aeronautics and Space Administration (NASA), to be used for space applications. However, the characteristics of the design are attractive for military applications as well.

Using high-assay, low enriched uranium (HALEU, between 5-20% enriched 235U), the uranium undergoes fission which in turn produces heat which is coupled to a LANL invention, an engine called a "heat pipe." The Lab summarizes the process simply:

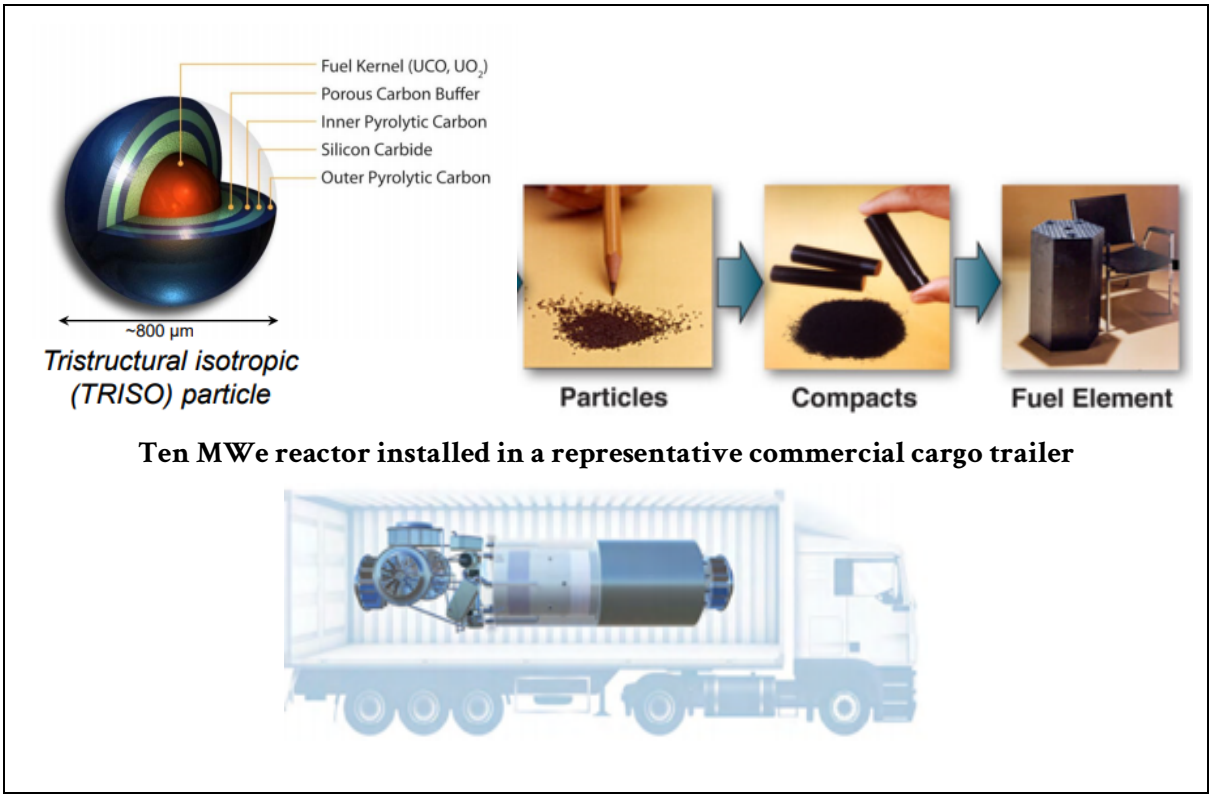
Whenever more power is needed, the heat pipe draws heat faster, cooling the reactor and therefore slightly shrinking the uranium. With the fissionable fuel now denser, the neutrons causing the chain reaction encounter more nuclei to split, thus increasing the reaction rate; in this way, the reactor automatically increases power when it's needed and, conversely, cuts power when it's not. This self-regulation also acts as a built-in safety guarantee.[9]

Unlike conventional nuclear power plants, which require large quantities of water for cooling, the LANL design requires no water or elaborate safety subsystems since the reaction of the fuel is self-limiting. When the temperature rises, the nuclear fuel expands, which stops the reaction.

If the reactor design is inherently safe, can the nuclear fuel be safe, particularly in a military environment? For two decades, the Department of Energy has sought a form of nuclear fuel that would be safe in new nuclear reactor design. The result was the development of the TRISO (tristructural isotropic) nuclear fuel particles shown below.

Each TRISO particle is composed of three layers: uranium, carbon and silicon carbide. The particle is less than a millimeter in diameter. These pellets—approximately 3,000 of them—are loaded into a 25 x 12 mm cylinder (known as a "compact"). In the reactor design, there are millions of the < 1 mm diameter fuel particles loaded into the fuel elements. The silicon carbide coating makes them highly heat resistant at temperatures that would cause steel to melt (~2500°F). The compacts are in turn loaded into hexagonal fuel elements and installed in the reactor, which will produce up to 10 MWe and operate for as long as ten years before requiring refueling. The entire system can be installed in a standard 40-ft commercial shipping

Figure 5: A Modern 10 MWe Transportable LEU TRISO Fuel-based Microreactor[10]



container for land, sea, or air transportation, as shown below.

These characteristics of the fuel particles, compacts, and fuel elements—and the lack of a requirement for a cooling system—make the reactor safe and highly proliferation resistant. Its compact and highly integrated design means it can be readily used in both civil and military applications. For example, in a small city of 150,000 (e.g., Santa Fe, New Mexico), ~40 MWe would be required to support the entire city's electric power needs. Thus, four reactors housed in shipping containers with power distributed through a modern microgrid could make the city independent of a larger regional or national grid.

Energy abundance is a game-changer for expeditionary campaigns, substantially mitigating the logistics burden associated with the transportation of liquids—fuel and water—which account for 80-90% of current needs. Converting energy-deprived expeditionary units into energy-abundant ones, and doing so in parallel to bases not involved in an expeditionary campaign, would be a remarkable change on several levels.

A closely-related institutional innovation that may contribute to the ability to rapidly field such nuclear energy systems is the integration from the outset of civil nuclear reactor licensing through the Nuclear Regulatory Commission (a 2.5 year-long process). By doing so in parallel with the development of the reactor, an early deployment of the capability would be possible. In March of 2020, the DoD's Strategic Capabilities Office awarded three contracts for competitive designs for the microreactors, with a plan for a 2027 completion date for Project Pele.

MILITARY IMPLICATIONS

Energy abundance is a game-changer for expeditionary campaigns, substantially mitigating the logistics burden associated with the transportation of liquids— fuel and water—which account for 80-90% of current needs. Converting energy-deprived expeditionary units into energy-abundant ones, and doing so in parallel to bases not involved in an expeditionary campaign, would be a remarkable change on several levels.

First, military effectiveness, agility, and resilience will be enhanced, while tactical vulnerabilities associated with the transport of liquids will be mitigated. At the same time, energy-intensive military applications such as high energy lasers, electromagnetic rail guns, high performance computing at the tactical edge, etc. will become appealing tactical and operational alternatives. Coalition operations with allied forces that lack expeditionary infrastructure will likewise be made practical by U.S. capabilities employed to provide tactical and operational support for electrical energy. Meanwhile, the tactical and operational "footprint"—and vulnerability—of U.S. forces will be significantly reduced by diminishing the need for large storage facilities, pipelines, and processing installations for liquids in main and forward operating bases.

The ability to transport the reactor system has important implications for U.S. bases at home as well. As is now well-known, the electric power grid and the entire information infrastructure are

vulnerable to both kinetic and non-kinetic attack. An adversary seeking to prevent the U.S. from deploying expeditionary forces from a major base or port in the U.S. might seek to attack the commercial power grid on which the base or port is dependent. The ability to transport this capability by land, sea, or air can both mitigate an important vulnerability and contribute to deterrence. Additional benefits can also be expected to accrue to in the context of U.S. disaster relief operations, since energy depravation is a nearly universal characteristic of natural catastrophes such as earthquakes, destructive storms, tsunamis, forest fires, and the like.

More fundamentally, the development, proliferation, and further expansion of microreactor technology could also upend the paradigm of electrification that has been in place for a century. Instead of having a few very large electric power generation sites connected through a grid, electric power generation could be significantly decentralized, making our power system more resilient, and providing heretofore untold flexibility in terms of our foreign and defense policy.

ENDNOTES

[1] Juan A. Vitali et al., "Study on the Use of Mobile Nuclear Power Plants for Ground Operations," Deputy Chief of Staff, United States Army, October 2018, 2,3, https://apps.dtic.mil/sti/pdfs/AD1087358.pdf (Table 2.1: Army Reactor Program – Portable/Mobile Reactor Systems)

[2] As cited in Jeff Waksman, "Project Pele Overview: Mobile Nuclear Power for Future DoD Needs," Office of the Secretary of Defense, Strategic Capabilities Office, March 2020, https://gain.inl.gov/GAINEPRINEI_MicroreactorProgramVirtualWorkshopPres/Day-2%20Presentations/Day-2-am.02-Nichols_PeleProgOverviewPublicMarch2020,19Aug2020.pdf; See also Greg Douquet, "'Unleash us from the tether of fuel,'" Atlantic Council, January 11, 2017, https://www.atlanticcouncil.org/content-series/defense-industrialist/unleash-us-from-the-tether-of-fuel/.

[3] Jeffrey B. Carra and David Ray, "Evolution of Petroleum Support in the U.S. Central Command Area of Responsibility," *Army Sustainment* 42, iss. 5, September - October 2010, https://alu.army.mil/alog/issues/SepOct10/petrol_support.html; "Pakistan 'to reopen key Nato Afghanistan supply route," BBC, October 9, 2010, https://www.bbc.com/news/world-south-asia-11507472

[4] D.M. Giangreco, "Artillery in Korea: Massing Fires and Reinventing the Wheel," U.S. Army Command and Staff College, n.d., https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/giangreco.pdf.

[5] Jeff Waksman, "Project Pele Overview Mobile Nuclear Power For Future DoD Needs," Office of the Secretary of Defense Strategic Capabilities Office, March 2020, https://gain.inl.gov/GAINEPRINEI_MicroreactorProgramVirtualWorkshopPres/Day-2%20Presentations/Day-2-am.02-Nichols_PeleProgOverviewPublicMarch2020,19Aug2020.pdf. (Slide: In A War Zone, Energy Logistics Are Critical)

[6] There is an extensive literature on this subject. See, for instance, Army Environmental Policy Institute, "Sustain the Mission Project: Casualty Factors for Fuel and Water Resupply Convoys," *AEPI Report*, September 2009, https://apps.dtic.mil/dtic/tr/fulltext/u2/b356341.pdf.

[7] Dorothy Robyn and Jeffrey Marqusee, "The Clean Energy Dividend: Military Investment in Energy Technology and What It Means for Civilian Energy Innovation," Information Technology & Innovation Foundation, March 2019, http://www2.itif.org/2019-clean-energy-dividend.pdf?_ga=2.218274393.1591902561.1609820375-566527249.1609820375

[8] Vitali et al., "Study on the Use of Mobile Nuclear Power Plants for Ground Operations." (Table 1.1: Energy Density)

[9] "Radiation Detection Gets Direction," Los Alamos National Laboratory *Spotlights*, February 2019, https://www.lanl.gov/discover/publications/1663/2019-february/_assets/docs/1663-33-RadiationDetection.pdf

[10] Blaise Collin, "AGR-5/6/7 Irradiation Experiment Test Plan," Idaho National Laboratory, January 2018, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_4446.pdf (Figure 3: Graphic of a typical TRISO-coated fuel particle); Hans D. Gougar, "Baseline Concept Description of a Small Modular High Temperature Reactor," Idaho National Laboratory, October 2014, https://inldigitallibrary.inl.gov/sites/sti/sti/6531061.pdf (Figure 1: TRISO fuel as loaded into a prismatic or PBR); "Radiation Detection Gets Direction," Los Alamos National Laboratory Spotlights, February 2019, https://www.lanl.gov/discover/publications/1663/2019-february/_assets/docs/1663-33-RadiationDetection.pdf

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

Ilan Berman	Chief Editor
Richard M. Harrison	Managing Editor, Layout
Alex Kim	Graphic Design

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 close to 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.

DEFENSE DOSSIER ISSUE 29

AMERICAN FOREIGN POLICY COUNCIL
509 C Street NE, Washington, D.C. 20002 | Telephone: 202.543.1006 | Fax: 202.543.1007 | www.afpc.org