OFFSET STRATEGIES TO **PREVAIL** AGAINST ASYMMETRIC THREATS

ASYMMETRIC THREAT SYMPOSIUM IX

On September 22, 2016, at the Gannett Conference Center in McLean, Virginia, the Association of Old Crows (AOC), CACI International Inc (CACI), and the Center for Security Policy (CSP) co-sponsored *Offset Strategies to Prevail Against Asymmetric Threats,* the ninth symposium in the Asymmetric Threats to National Security series.

This document is intended only as a summary of the personal remarks made by symposium participants and symposium discussion themes and is published as a public service. It does not necessarily reflect the views of AOC, CACI, CSP, the U.S. government, or their officers and employees.

Note: The content of this report reflects the invocation of the Chatham House Rule for the symposium and report as non-attributable forums.

TABLE OF CONTENTS

The pro bono Asymmetric Threat symposia series was initiated by CACI in 2008 to contribute to the national discourse on the topic of asymmetric threats facing the United States.

EXECUTIVE SUMMARY

ASYMMETRIC THREAT SYMPOSIUM IX

OFFSET STRATEGIES TO PREVAIL AGAINST ASYMMETRIC THREATS

On September 22, 2016, the Association of Old Crows, CACI International Inc, and the Center for Security Policy hosted "Offset Strategies to Prevail Against Asymmetric Threats," the ninth in a series of symposia on asymmetric threats. The event featured a wide-ranging discussion on how to address the complex asymmetric threats to America's national security and how offset strategies attempt to position the U.S. to prevail against resurging global power competition, multi-regional conflicts, and cross-domain challenges. The symposium was held under the Chatham House rule of non-attribution.

Threats against the United States have become increasingly complex and diverse, involving nation-states and non-state actors, conventional and unconventional tactics, and a wide variety of weapons. These asymmetric threats have proliferated against the backdrop of a leveling of the technological playing field, along with convoluted acquisitions processes that make it difficult for the U.S. to rapidly field new solutions. The U.S. operates in a highly volatile global environment, beset by regional conflicts, the global war on terrorism, political and economic disruptions, cyber attacks against the homeland, and disease pandemics. With U.S. strategic superiority being challenged, the Department of Defense is proposing a bold solution in the form of an offset strategy.

The first offset strategy was the early Cold War endeavor to counteract the Soviet Union's quantitative superiority by developing a formidable nuclear arsenal. Even long after the Cold War, this strategy continues to sustain the safety of the U.S. and its allies. America's conventional forces are able to operate because there is a nuclear umbrella over them composed of the "triad" of intercontinental ballistic missiles, submarine-launched ballistic missiles, and bombers. And while Russia, China, and North Korea aggressively sustain and build their arsenal, Iran continues its pursuit of a nuclear weapon. In this environment, the U.S. can ill afford to lag in modernizing its nuclear arsenal as well as its command and control capabilities.

The second offset strategy was pursued in the 1980s to develop a new generation of stealth technologies, precision-guided weapons, and complex command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities.

The third offset strategy includes manned-unmanned teaming technologies to transform and prepare the military for multi-regional conflicts and cross-domain challenges. In pursuing a countervailing strategy, the U.S. must adopt an interagency approach in response to adversaries avoiding strictly military engagements to gain a strategic advantage. A successful strategy should also reach out to the private sector. However, laws and regulations have not kept pace with the advancement of technology. The legal authorities are not in place to facilitate multiple federal agencies acting in coordination with private entities, such as commercial power plants, telecommunications providers, and financial institutions, in the event of a catastrophic occurrence like a terrorist attack.

Investing in game-changing technologies to outpace increasingly dynamic globally fielded systems and anti-access/area denial (A2/AD) developments are core components of this strategy. At the forefront are autonomous systems, which enhance the capability of U.S. forces to deal with the scale, speed, and complexity of today's advanced technologies and variety of threats.

An offset strategy is necessary to preserve the security of the U.S. against increasingly diverse, complex, unprecedented threats.

To what degree the U.S. gives fuller authority to weapons systems or decision aids is still dependent on the evolution of the technology, and the ethics and legality of allowing autonomous systems to make decisions without human intervention.

Morality demands maintaining a human in the loop for lethal effects, though U.S. adversaries may share no such scruples. Strategic thought is necessary to define where to apply human-machine teaming, and under what circumstances autonomous systems might be allowed to detect and defend without human intervention in order to prevent catastrophic attack on a level too large, fast, or complex to accommodate human response time, such as a cyber or electronic warfare attack.

Unmanned aerial and other robotic vehicles continue to play a large role in yielding a disproportional advantage across the full spectrum of today's battlespace, primarily as a result of their capability to provide 24/7 global coverage at significantly reduced costs. In 1996, the U.S. had a single continuous orbit of unmanned aerial vehicles (UAVs). Today, we are approaching 100 around-the-clock orbits of UAVs. Of equal importance are information-processing systems that can digest and find patterns in vast amounts of data. These systems are critical to achieving the strategic edge through decision speed and superiority.

Technological advancement also requires new strategies for cooperating within the services themselves. The Air Force is advancing Enterprise Capability Collaboration Teams to bring together the major commands, science and technology (S&T), and acquisitions communities, enabling teams to close user-identified operational gaps by developing weapons systems that incorporate S&T innovation.

Investment in technologies and the legal authorities to facilitate private sector coordination must acknowledge that America's commanding technological edge is eroding. Unprecedented access to U.S. innovation has resulted in exploitation via espionage, cyberspace, and open networks. China, already outpacing the U.S. in science, technology, engineering, and math (STEM) Ph.D. education by two to one, has surpassed the European Union in research and development investment and is closing in on the U.S.

In order to close the technology gap, the U.S. must pursue agile and adaptive acquisitions processes. Reducing time to market with solutions that are adaptable upon delivery to meet changing mission requirements is key. Furthermore, adversaries are developing countermeasures faster than we can field systems. To prevail, we must develop globally interoperable systems built on open architectures, which avoid the impediment of vendor lock or allied consensus to be compatible with their capabilities.

The nation's acquisitions process must also allow for developing systems to a point where they meet immediate mission requirements, while leaving flexibility to further optimize these systems based on the parameters of specific future missions. Finally, deferred fielding of solutions without commitment to a particular system or interrelationships gives the U.S. the flexibility to incorporate future updates as technology continues to evolve.

An effective strategy should consider all available resources and incorporate lessons learned across the interagency. For example, the success of the Drug Enforcement Agency in achieving a strategic relationship with the National Security Agency and other agencies to bridge intelligence gaps with law enforcement communities in combatting narcoterrorism may serve as an example for building cooperative relationships to counter asymmetric threats.

As nation states and terrorists become bolder in their actions, interagency collaboration with local law enforcement could further enhance U.S. strategic capabilities. The FBI estimated there were 1,000 open investigations into terrorism in the U.S. in June 2016. Improved lines of communication and collaboration

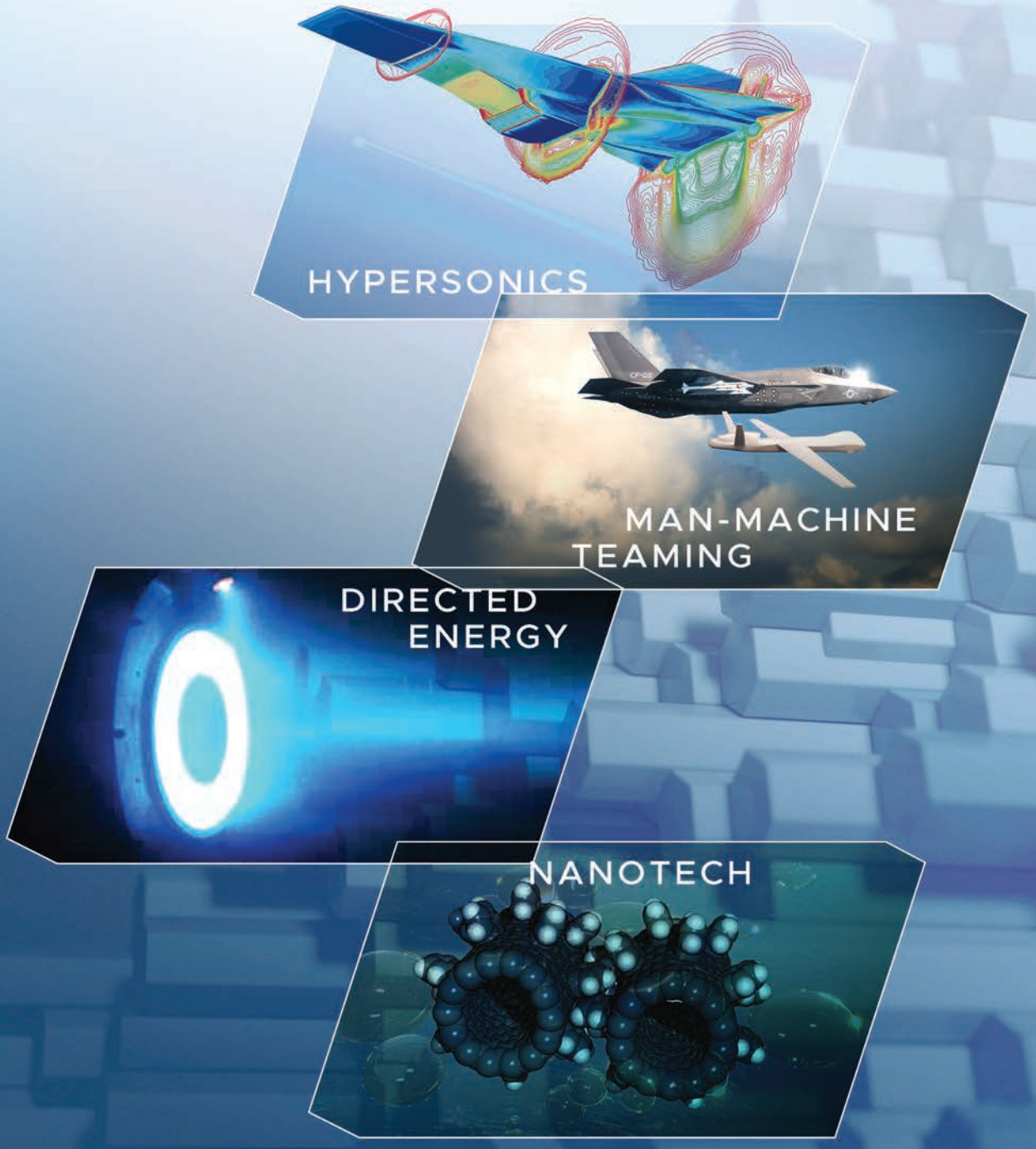
▲ **National security strategies seek to countervail increasingly diverse, multi-regional asymmetric threats.**

Photos by Vitaly V. Kuzmin and Uri Tours

with the nation's 800,000 state and local law enforcement officials would exponentially expand the ability to avert or respond to a terrorist incident at both of these levels of government.

In today's threat environment, the concept of an adversary has grown ambiguous. The fundamental goal of the countervailing strategy is to create long-term, sustainable advantages. The offset is a response to many adversaries, some defined by geographic boundaries, others by ideological ones. It also makes the principle of never being constrained to a "fair fight" even more important. The pursuit of this strategy is necessary to preserving the security and prosperity of the U.S. against unprecedented threats.

1 Why Is an Offset Strategy Needed?



The global threats the United States and its allies face have become increasingly diverse and complex. Adversaries employ a wide variety of weapons, from the makeshift to the sophisticated, along with conventional and unconventional tactics. Participants range from non-state actors to nation states and span the ideological spectrum. New threats emerge against the backdrop of the nation's diminishing technological advantage. These asymmetric threats have reduced America's strategic advantage at a time when defense budgets are shrinking and complex acquisition policies stall the fielding of new capabilities. To compensate for this adversely changing power dynamic, the Department of Defense (DoD) has turned to an idea out of the past: the offset strategy.

This strategy relies on bolstering innovative technologies and policies at a time when the U.S. faces a highly volatile and diverse threat environment. Global terrorism has become more pervasive than ever, while Iraq and Afghanistan remain active combat zones even after the major drawdown of U.S. troops. Russia and China are investing in the outcomes of such destabilizing conflicts as the Syrian civil war. North Korea and Iran are escalating ballistic missile testing, as China continues to assert itself in the East China and South China Seas.

In addition to these military threats, the world faces significant political and economic upheaval. U.S. social unrest has galvanized tensions between minority communities and police. Furthermore, global disease outbreaks such as Ebola and the Zika virus test the world's responsive capabilities.

With the increasing prevalence, diversity, and complexity of global asymmetric threats, it is imperative that the U.S. put forth a strategy that allows it to retain the freedom to attack and the freedom from attack in and through all domains – air, sea, land, space, and cyber – as well as across the electromagnetic spectrum. An effective and efficient integration of systems, capabilities, operations, and policies will require multi-dimensional approaches that are nuanced and innovative. The offset strategy is one such approach, largely focused on manned-unmanned teaming technologies, to transform and prepare the military for multi-regional conflicts and cross-domain challenges.

The evolution of the offsets is interwoven with the evolution of modern warfare. World War I saw massive military and civilian casualties. During this period, significant technological advancements were made in military resources, including the tank, airplane, submarine, and machine gun, as well as the telephone and telegraph. World War I was called the "war to end all wars," and the fallacious assumption in this phrase was that the technological and material superiority this war engendered could deter future conflict on such a vast scale.

For example, after World War I, the French developed the Maginot Line, a series of fortifications along the French side of its borders with Switzerland, Germany, and Luxembourg. But in World War II, the Germans responded with the "Blitzkrieg," a "lightning war" that completely circumvented and penetrated the Maginot Line.

In World War II, some 60 million people were killed, equaling approximately 3 percent of the world's population at the time.[1] Afterward, an offset strategy was advanced: an early Cold War-era plan to leverage nuclear capabilities to compensate for the Soviet Union's significant quantitative advantage in conventional forces. However, the nuclear offset was not a means to end all conflict. While our conventional forces were able to operate because of the nuclear umbrella over them, the same could be said of Russia. The evolution of mutually assured destruction (MAD) created the ultimate symmetry.

Since the advent of nuclear deterrence, wars, skirmishes, and police actions – even the global war on terrorism – have yielded casualties that

1 "By the Numbers: World-Wide Deaths," The National World War II Museum, http://www.nationalww2museum.org/learn/education/for-students/ww2-history/ww2-by-the-numbers/world-wide-deaths.html; "Historical Estimates of World Population," U.S. Census Bureau, https://www.census.gov/population/international/data/worldpop/table_history.php.

are, while still significant, a much smaller fraction of the world's population. The crucial role that nuclear capabilities continue to play is that there have been no global wars because the outcome has not been worth the risk by nation states. However, it is important to consider that this assumption is not valid for ideologically-driven movements, such as radical Islamic terrorism.

The nuclear deterrent is essential to keeping the U.S. and its allies safe. In order to achieve the desired deterrent effect, nuclear capabilities must be backed by credible delivery systems. These consist of the "triad" of technologies conventionally defined by intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles, and bombers with nuclear weapon delivery capabilities.

▼ **The Cold-War era offset strategy of nuclear deterrence that contributed to the fall of the Berlin Wall is still foundational to keeping the U.S. and its allies secure.**

The necessity of a responsive and flexible triad is critical. The value of the ICBM leg of the triad is that it yields a high level of responsiveness to protect the U.S. and maintain the strategic value of preemptive strike options. The nuclear submarine still provides the most survivable capability, although it is constrained by limited resupply options. The virtue of the bomber is its flexibility to project force anywhere in the world, be easily recalled when tensions subside, and use stealth effects to reduce vulnerability while extending second-strike capability.

The need to modernize the triad is predicated on the defensive attributes it provides to counter an increasingly assertive Russia, China, Iran, and North Korea, as well as non-state actors seeking to acquire nuclear weapons. While some emerging threats lack the resources and strategy to achieve the delivery systems necessary to match the nuclear capabilities of the U.S., peer competitors Russia and China are aggressively modernizing or developing effective systems. The U.S. must keep pace to sustain the strategic "checkmate" of credible first-strike and retaliatory potential against nuclear peers.

The deterring effect of the U.S. nuclear force pushes the need to deter other immediate, dynamic, and evolving threats. The current offset strategy is largely focused on bold innovations such as manned-unmanned teaming to transform and prepare the military for multi-regional conflicts and cross-domain challenges. Over the next five years, DoD plans to invest $28 billion into six emerging areas: anti-access and area-denial (A2/AD), guided munitions, undersea warfare, cyber and electronic warfare, human-machine teaming, and war gaming and testing new operating concepts.[2]

In pursuing a countervailing strategy, the U.S. must ask: What is its Maginot Line of defense? What are its blind spots? There is clearly an urgent need for idea challenging and creative analysis. As to

---

2 Stephen Welby, Assistant Secretary of Defense for Research and Engineering, statement before the Subcommittee on Emerging Threats and Capabilities, Armed Services Committee, United States Senate, April 12, 2016.

The U.S. must retain the freedom to attack and the freedom from attack in and through all domains.

vulnerabilities, the cyber domain certainly presents serious concerns. Protecting networks is now as fundamental as protecting airfields, battalions, surface ships, and civilian centers. Furthermore, a generation of officers came of age during the 1990s, when the convention was permissive access. Yet A2/AD is entrenched in today's global battlespace. The evolution of peer competitor and adversary weapons systems of greater reach and increased precision has expanded contested environments.

Other nations have observed the way the U.S. fights wars. They will not grant it time to move ships, unload equipment, set positions, and attack. Future warfare will involve rapid fielding of mission-critical systems, which will require agile and adaptive acquisition strategies.

The tenets of warfare are being rewritten. This is most evident in the global war on terrorism. The Islamic State, in publishing its lessons learned from the attack on Nice, France, has described its strategy: softer targets, diverse weapons systems, and different techniques. Radical Islamic terrorism has upended our concepts of warfare. Its ideology is proliferated by exploiting social media and its funding is largely generated by narco-trafficking and untraceable financial sources. Defeating such an adversary requires a strategy that spans national defense, law enforcement, and the private sector.

Radical Islamic terrorism adds a further dimension of complexity in that it both provokes and prospers from regional destabilization in unanticipated ways. For example, the influx into Europe of hundreds of thousands of refugees displaced by the Syrian civil war has created a level of uncertainty, disorder, disharmony, and chaos upon which terrorism thrives.

It is clear that a countervailing strategy must take into account an increasingly volatile global context. This strategy should ensure that the U.S. maintains its strategic advantage against conventional threats, while boosting its capability to deter and defeat asymmetric, atypical, unconventional, multi-domain adversaries worldwide. A significant component of such a strategy is creating and implementing innovative technologies and operational concepts. However, considerations must extend beyond new technologies to encompass what strategies might succeed against diverse threats, from supporting Ebola and Zika pandemic response to combatting terrorism; from cyber attack to conventional conflict and escalating nuclear responses.

▼ **The second offset strategy yielded stealth technologies, precision-guided weapons, and complex C4ISR used to achieve overwhelming success during the Gulf War.**

2 Finding, Forging, and Fielding Offset Technologies, Capabilities, and Operational Concepts

The United States is experiencing a new generation of warfare where its national security advantages are tested in every dimension and at the strategic, tactical, and operational levels. America's competitive strategy depends on projecting forces, fielding technologically superior weapons and systems, and retaining the strategic initiative. There is an intimate link between technology and capability, just as there is between strategy and concept of operations. The U.S. has decided to reenergize and invest in technologies that are increasingly multi-domain, dynamic, and adaptive, as well as capable of A2/AD responses.

Prospective game-changing technologies include hypersonic weapons and aircraft that travel faster than Mach 5, making them difficult to shoot down and increasing the distances in which they can effectively penetrate adversary A2/AD environments. Another promising area is directed energy, which includes both high-powered lasers and high-powered microwaves capable of debilitating an adversary's electronics systems. Nanotechnology has already begun to transform how the U.S. engineers equipment and manages logistics.

A flexible, multi-disciplinary countervailing strategy should apply an interagency approach to integrating new technologies and operational concepts across defense, intelligence, federal law enforcement, and other federal agencies. Such an approach should also bring in the private sector, increasingly targeted by adversaries and nation states for the purpose of endangering communications, energy, transportation, infrastructure, and financial institutions.

An effective countervailing strategy should impel coordination not only across government and the private sector, but within departments themselves. For instance, the Air Force is advancing a new approach involving Enterprise Capability Collaboration Teams focused on multi-domain challenges to enhance cooperation among the science and technology, acquisitions, and user communities. Here, stakeholders

In today's battle environment, the speed, accuracy, and quality of decisions govern the magnitude of success.

come together to determine capability gaps among the military commands and identify technologies that can fill these gaps.

This new approach recommends reinvigorating the enterprise process to make the leap from basic and applied research by promoting experimentation, modeling, simulation, prototyping, and analysis to advance bold capabilities. The ultimate goal is to expedite the development of systems and strategies across government and the private sector that meet the warfighter's requirement to quickly adapt and evolve in order to maintain a battlefield edge against asymmetric threats.

Interagency coordination with the private sector opens a host of possibilities for integrating new technologies. The combat cloud is a prime example of private sector technology successfully adapted for military application. It has enabled the U.S. military to securely move warfighting information out of individual platforms to a cloud-based computing system, where it can be shared by multiple, cross-domain platforms. Conversely, there is a great deal of hand-off from the government to private industry in such high-potential areas as space launch, which is likely to accelerate in years to come. For example, Google plans to put 4,000 satellites into space to gain world coverage, a capability of limitless value to DoD.[3]

It should be kept in mind that commercial technologies carry inherent risk. DoD is highly dependent on numerous commercial systems that are going to have the Internet of Things (IoT) woven

3 Dominic Gates, "Elon Musk Touts Launch of 'SpaceX Seattle,' " *The Seattle Times,* January 16, 2015, http://old.seattletimes.com/html/businesstechnology/2025480750_spacexmuskxml.html.

▲ **Autonomy speeds decisions and acts as a force multiplier – for example, enabling a "swarm" of UAVs to accompany a piloted aircraft.**

throughout their entire infrastructure and fabric of operation. But the composite IoT devices are too small to host encryption or to receive patches, opening an array of security vulnerabilities.

A key technology of countervailing strategies is autonomous systems. Autonomy enhances the capability of U.S. forces to deal with the scale, speed, and complexity of today's systems, platforms, and information. Cyber warfare requires sub-millisecond response times that can be impeded by a human operator in the loop. These systems also act as force multipliers – for example, enabling a single pilot to be accompanied by a "swarm" of autonomous aircraft.

Their importance is not lost on U.S. adversaries, either. In Syria, every participant, from the U.S. to the Russians, to Assad's regime and the Syrian rebels, is using unmanned aerial vehicles.

As systems continue to grow more complex and networked across domains, the capability of autonomous systems to collect, analyze, and find patterns in vast, disparate information offers critical decision support. These systems will incorporate both "autonomy-in-motion," which is the physical presence (i.e., robotics, satellites, UAVs) and "autonomy-at-rest," which operates virtually (i.e., planning and expert advisory systems or operations centers).

The possibilities that autonomous systems offer in this area may compel us to re-envision the function of our military services. In today's battle environment, the speed, accuracy, and quality of decisions govern the magnitude of success. For this reason, defense and intelligence agencies might benefit by thinking of themselves as information-processing, knowledge-intensive service organizations with diverse peripherals, whether they be satellites or submarines or aircraft.

In referring to potential innovation, it is critical not to be boxed in by thinking only of technology – software and hardware, networks, platforms, equipment. Legal authorities, for example, can enable interagency coordination with the private sector to advance strategic initiatives.

The recurrent dilemma the U.S. faces is that it does not have the legal authorities in effect that enable an interagency approach that engages the private sector. Simply put, regulations have repeatedly failed to keep up to evolving technologies, as well as their applications and arrangements. This point is especially salient when considering that the target of asymmetric threats is often the private sector itself.

Consider the position of the chairman of a major telecommunications provider solicited by a federal agency to use the company's network for a military action or to preempt an attack. Such scenarios and questions have likely not been broached at the board level or in the executive suites as to what access, if any, the company could legally allow or how it would respond.

With this in mind, the Joint Interagency Combined Space Operations Center is developing new space system tactics in response to increasing threats to vulnerable space capabilities.[4] The initiative will unify effort and facilitate information-sharing by operationally integrating DoD and intelligence space communities, as well as civil, commercial, allied, and international partners.

It is critical to evolve today's thinking about such topics as takeovers of networks, information-sharing with private sector companies or foreign governments, military and intelligence interactions with corporations, classified solutions on unclassified networks, electronic espionage, and the linkage between economic and national security.

A framework of legal authorities across military force and business processes, laws and treaties, departmental regulations, and statutes is necessary to facilitate cooperation and integration of the private sector with military and other interagency operations. Failure to achieve this symbiosis may lead to disastrous consequences if the U.S. is faced with a large-scale attack on its private sector.

▼ The combat cloud is an example of a private sector technology adopted by the military to enable information-sharing across the interagency.

4 U.S. Strategic Command Office of Public Affairs, "New Joint Interagency Combined Space Operations Center to Be Established," Department of Defense, Sept. 11, 2015, http://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established.

3 What Offset Strategies Assure Operational Success Against Asymmetric Threats?

Before the United States can decide what offset strategies contribute to operational success, it is important to remember why there is a need for the next offset. The U.S. does not want to find itself in a "fair fight" against an enemy that may be larger in size or less constrained by resources or ideology. Throughout the Cold War, nuclear weapons, precision-guided munitions, and stealth technology proved successful in deterring conflict with the Soviet Union, but the U.S. no longer has a defined adversary with a regimented order of battle.

Regardless of who future adversaries will be, the operational approach must be to regain the commanding technological advantage the U.S. once held. Since the Persian Gulf War, other countries and adversaries have keenly observed as the U.S. employed stealth technology and precision-guided munitions. They took note of its reliance on the Global Positioning System for navigation and targeting. They sought vulnerabilities in its complex command and control networks across all domains. As peer states invested in technology and capabilities, the Islamic State and other terrorist organizations subverted the U.S. technological advantage by leveraging the power of social media to recruit and communicate, sometimes hiding their activities here under the legal protections of U.S. privacy laws. With constrained financial resources, the U.S. must focus less on specific capabilities and more on how it can rapidly identify, develop, and employ solutions to offset emerging threats.

This starts with a renewed national emphasis on growing the next generation of scientists and engineers. The innovative edge will be best maintained by investing in science, technology, engineering, and math (STEM) education even at the earliest levels. The lifelong immersion of these younger generations has already led them to use and think about technology in novel ways. Of added significance is how technology has influenced young people's viewpoint of secrecy and privacy in the context of national security.

▲ **The U.S. education system provides foreign students with access to esteemed universities without reciprocal return.**

It must also be acknowledged that America's lagging STEM performance may obstruct developing this potential innovation and talent. The U.S. educational system provides foreign students with access to the nation's most talented university professors and national research labs. These students then take their knowledge back to their home countries. One result is that China is estimated to produce twice the number of STEM Ph.D.'s than the U.S.

Given fiscal and physical constraints, it is not possible to deploy overmatching capabilities or countermeasures against every threat. Furthermore, the current acquisitions process is cumbersome and impedes game-changing technology. Technology that does make it through the entire process to become a program of record is often late to address the need, or excessively expensive to modernize and adapt to changing missions. Instead, the U.S. must exploit adversaries' capability gaps more rapidly with an agile and adaptive acquisitions process.

American eagerness to pursue perfection has steadily increased time to market for new technology.

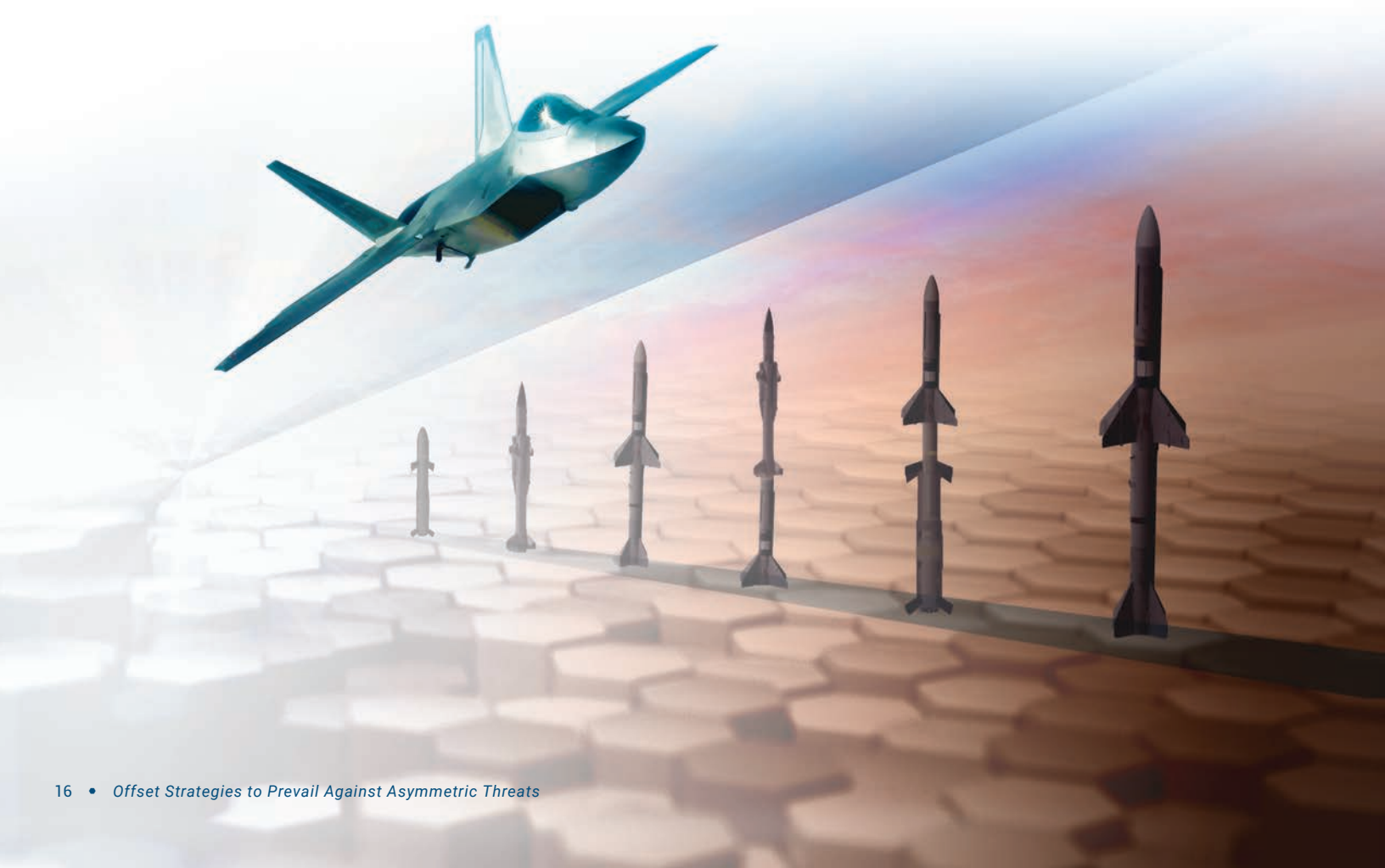
One consequence of complicated acquisitions processes and lagging STEM education is that DoD simply does not have sufficient numbers of qualified engineering professionals to work on certain critical development programs. The military services used to have depth in engineering departments. This lack of expertise constrains the services to drafting requirements that are unnecessarily detailed because they are not confident in their ability to fix or re-engineer solutions when delivered.

Every change in requirements or evolution in mission requires the service to return to the prime contractor. Besides the higher associated costs, the resulting delays give adversaries the opportunity to evolve their countermeasures to match or defeat our new capabilities.

Due to talent shortages and budget constraints, the U.S. is losing the authoritative lead it once held in research and development, while China is emerging as a most worthy competitor at an alarming rate. Over the past several decades, China progressed from modest investment in research and development to become the second highest global spender behind the U.S.[5] China is

5 National Science Board, *Science and Engineering Indicators 2016,* National Science Foundation, January, 2016, https://www.nsf.gov/statistics/2016/nsb20161/#/.

▼ **Russia evolved six generations of surface-to-air missiles in the time it took the U.S. to develop and deliver the first F-22 Raptor.**



making this investment across the full spectrum of technology, rapidly closing the technological gap.

With the U.S. military encumbered by a tedious acquisitions process, adversaries are developing countermeasures to defeat the most advanced capabilities faster than we can field them. American eagerness to pursue perfection, when simpler solutions delivered faster and in greater quantity might have been the optimal solution, has steadily increased time to market for new technology. Russia evolved an air defense for the F-22 Raptor faster than the aircraft could be developed, fielding six generations of surface-to-air missiles in the time it took the U.S. to deliver the first fighter.[6] Insurgents continually modify relatively low-cost improvised explosive devises to counter U.S. advances in tactics, techniques, procedures, and armor technology.

One approach to decreasing time to market is to develop systems that are globally interoperable but do not require global consensus. Industry partners, U.S. military services, and coalition countries are often limited by their ability to transmit information to each other because they operate on different proprietary systems that are incapable of interfacing with each other. By moving to systems and platforms based on open network architecture, it will no longer be necessary for all parties to reach consensus on the capabilities their connected systems will provide or how these systems will interact.

Open network architecture also provides the added benefit of reducing impediments to fair and open competition. Inflexible government standards and reliance on proprietary software, platforms, and systems frequently means that small businesses cannot compete to provide even small components or sub-systems. The government loses the ability to compete new requirements because it has to resort to the prime contractor for modifications to a proprietary system. Globally

▲ **B-52 Stratofortress with armament of conventional bombs, precision-guided munitions, and nuclear warheads.**

interoperable systems provide an interface that allows multiple proprietary systems to interact with the open platform and with each other without exposing proprietary information.

A second way to speed up acquisitions is to "compose then optimize." The current design process focuses on building an excellent system, but is the U.S. allowing "great" to be the enemy of "good"? A more effective strategy might be to develop a system up to a point of functionality, but leaving room for additional design freedom. Services could then field it faster, potentially at lower cost or greater numbers, then optimize the composition based on particular mission parameters. Instead, the quest for a perfect solution often consumes more funding than planned and the final quantity delivered is far fewer than originally programmed.

6 Megan Chuchmach, Lee Ferran, and Mark Schone, "Final F-22 Fighter Delivered, McCain Says $79B Jets Still Have No Mission," *ABC News,* May 3, 2012, http://abcnews.go.com/Blotter/final-22-fighter-delivered-sen-john-mccain-79b/story?id=16270127.

▲ **Legal authorities must account for fully autonomous and interagency responses.**

This acquisition investment strategy involves creating platforms that leave enough design room to be optimized for multiple purposes, similar to the B-52 that has supported missions ranging from nuclear deterrence to saturation bombing to delivery of precision-guided munitions and close air support. New platforms must allow for competition over the lifecycle for replacement components and modernization. They must be able to accept and integrate IT systems that will be continually updated. With over 30 percent of the military turning over every year, the IT systems need to be as intuitive as a smartphone to reduce or even eliminate the amount of training required.

Composing then optimizing helps achieve better "float and flow," or deferring technical decisions until as late as possible without committing to any system or interrelationships. The F-22 Raptor is a prime example of a system that the service committed to before there was a clearly articulated capability gap to fill.[7] There are significant consequences that are often not considered when committing to major long-term investments or rapid solutions. Once the commitment is made to move forward, that investment will dominate or affect the time to market of other technologies. There will be less funding and talent available for research and development of other projects.

In taking active steps to reduce time to market, the U.S. must define and address legal and moral constraints that affect how it acquires and deploys capabilities. In the instance of autonomous systems generating lethal effects, morality demands a human in the loop. However, the U.S. must also prepare for the probability that its adversaries will not hold themselves to the same moral standards.

To avoid being vulnerable to fatal attack capabilities, it is essential that America's moral standards, legal authorities, and frameworks empower, not constrain, the U.S.'s ability to protect itself. Agencies will have to clearly identify and obtain the necessary legal authorities in advance for a fully autonomous and interagency response to certain scenarios. Attacks against infrastructure, communications, or transportation networks could have such catastrophic consequences that an autonomous response may be the only viable option. Human beings simply cannot process information fast enough to detect, decide, and react to a large-scale cyber attack, for example.

The U.S. also needs a greater ability to protect research and development efforts. The nation's legal frameworks, combined with its open society, have created an environment where technologies that can be employed against emerging threats are

7 Ibid.

Human beings cannot process information fast enough to detect, decide, and react to a large-scale cyber attack.

not used because they would potentially have to be disclosed through federally regulated tests and evaluation that adversaries may be able to access. Trial evidence that becomes public information also provides key sources of intelligence on U.S. technology, tactics, and procedures.

Given the diversity of today's threat environment, the U.S. must be open to innovative strategies that employ unconventional tactics, consider all possible targets, and pursue a high degree of coordination. It has to understand and disrupt, for example, adversary communications and finance networks via an interagency approach that demands larger-scale collaboration. This will require applying best practices learned from agencies DoD is not accustomed to collaborating with on a broad scale.

There are also lessons to be learned from combatting transnational crime and narco-terrorism. The Drug Enforcement Agency (DEA) struggled for years to penetrate and defeat Pablo Escobar's cartel because the necessary collaborative interagency approach was not in place. To combat narco-trafficking, the DEA created a Special Operations Division through a strategic relationship among the DEA, the National Security Agency, and other agencies to bridge intelligence gaps with law enforcement communities. Through collaborative efforts, DEA and local law enforcement developed the cohesive tissue to share and understand intelligence information without compromising each organization's ongoing investigations.

The same concepts are applicable to defeating asymmetric threats from non-state actors. As terrorists become bolder in their actions, collaboration between intelligence agencies and local law enforcement has to improve. In June 2016, the FBI Director assessed that there were 1,000 open investigations into terrorism in the U.S.[8] However, the FBI's 17,000 federal agents are also consumed fighting a host of other federal crimes and do not have the resources or perfect intelligence to act on every lead. Collaboration with the nation's 800,000 state and local law enforcement officials can exponentially expand federal law enforcement's network and improve its ability to avert or respond to a terrorist incident. The speed at which law enforcement caught the Boston Marathon bombers, and more recently the New York and New Jersey bombers, is testament to the effectiveness of a coordinated effort.

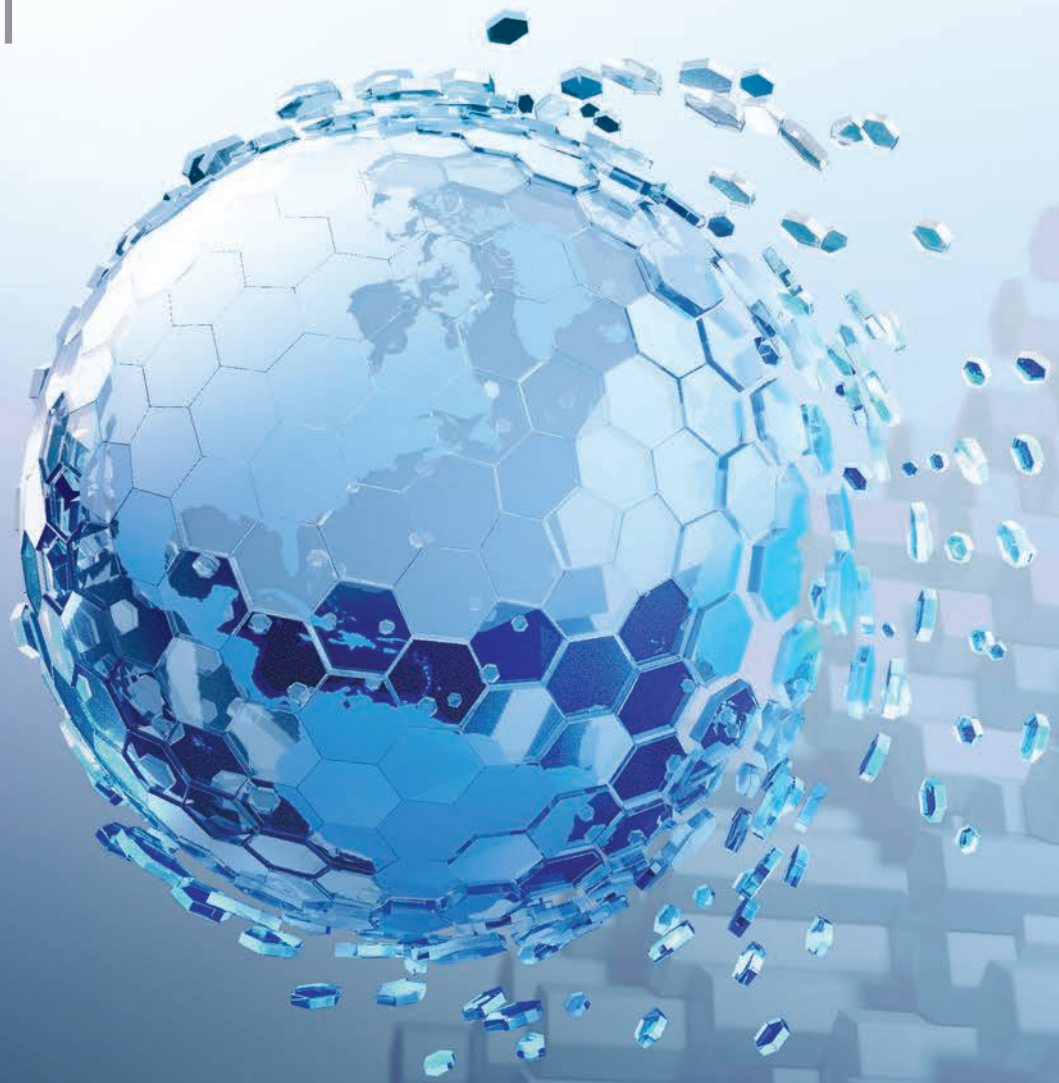
While some challenges in today's threat environment may be new, the will to win and to defeat the enemy has always been the same.

The early offset strategies created and sustained the Cold War-era condition of "mutually assured destruction" that resulted in 50 years of relative peace between two superpowers. Can the U.S. achieve the same ends with offset strategies based on cyber warfare and autonomous systems and an increasing threat from non-state actors?

Going forward, the U.S. has to consider two distinct strategic differences between past and current threat environments. First, it is no longer deterring or defeating only nation states. Second, it may be constrained in its ability to demonstrate the resolve to deploy a game-changing capability. When the U.S. used nuclear weapons to end World War II and employed stealth and precision-guided munitions in Operation Desert Storm, its adversaries knew it had the capability and was willing to use it. Non-state actors fighting for ideologies may not respond to this kind of deterrence. When confronting nation states and non-state actors, the U.S. has to be clear on the conditions, and demonstrate the will to win by crushing and defeating the enemy.

8 The Associated Press, "FBI Director: Number of ISIS Cases in US Has Not Dropped Off," June 7, 2016, http://www.newsmax.com/Newsfront/comey-fbi-isis-cases/2016/06/07/id/732802/.

4 Conclusions



In pursuing countervailing strategies against asymmetric threats both old and new, the United States must invest in game-changing technologies and transformative concepts and approaches to prepare the military for multi-regional conflicts and cross-domain challenges. Autonomous systems and human-machine teaming command the innovative forefront of U.S. offset strategy, as the rapidly escalating speed, scale, and complexity of systems tend to push humans further and further out of the decision-making loop.

However, by focusing on human-technology integrated tools and concepts, is there a risk of eliminating the human factor? Autonomous systems are being designed to make critical – even lethal – decisions without human intervention. National and international laws, regulations, and discourse must address the legal and moral questions raised by such technological advancements. These discussions could fundamentally redefine internationally accepted laws of war as robotics and autonomous systems become more prevalent on the battlefield. Nonetheless, an overarching condition that must be addressed is the absolute requirement to prevail in any and all warfare scenarios.

In the end, with the boundaries of autonomy expanding, the U.S. should not forget that warfare is a human endeavor. Often the outcome is determined by the will of the adversaries. Where lethal force may be needed, morality compels us to keep a human involved.

America's adversaries may not share this constraint. For the U.S., then, the speed of decision is critical. Human-machine teaming affords the opportunity to dramatically reimagine the form and function of services as information-processing, knowledge-intensive service organizations, which can turn vast data into knowledge that drives decisions significantly faster than an adversary can act.

The U.S. cannot abide a continued leveling of its technological edge. With China sprinting

In the end, with the boundaries of autonomy expanding, the U.S. should not forget that warfare is a human endeavor.

to close the technology gap between itself and the U.S., reinvigorating applied research and development would help reverse the erosion of the commanding technological lead the U.S. previously enjoyed. Cyber warfare and security is another critical area, as U.S. technologies are freely plundered through cyberspace, and as adversaries exploit the gaping holes in an open Internet.

DoD has spoken in detail about the offset's technological and spending priorities. Yet by doing so, has the U.S. either inadvertently or knowingly exposed its vulnerabilities? Furthermore, has the nation shown its opponents what they should plan to deter, counter, or destroy?

Unfortunately, threats are evolving much faster than the U.S. can build systems. To this end, it must pursue an agile acquisition strategy that decreases time to market for emerging technologies. Innovation cannot be allowed to stagger through long development cycles while requirements speed past.

One solution is to employ an open architecture-based development approach that allows for global interoperability without demanding global consensus. This includes the pursuit of more "good-enough" platforms in greater quantity and lower cost, with intentional design freedom to subsequently optimize the system for specific missions. Open architecture allows deferring commitment to a particular configuration until a clearly defined, mission-specific requirement has been identified. Open architecture-based platforms also break down barriers to entry for small, innovative, and entrepreneurial businesses while allowing established contractors to

protect proprietary information. These flexible architectures create open and fair competition for modernization across the platform lifecycle. They also enable rapid insertion of significantly mature technologies developed by the original equipment manufacturer or other industry providers.

Flexibility must also extend to developing the legal authorities necessary to facilitate interagency cooperation and engage the private sector. The rules, regulations, and statutes are not now in place to integrate military and commercial capabilities. This reality may pose dire consequences when considering that a significant asymmetric threat to the U.S. is an attack on the private sector – the hub of its national economic stability.

Fielding effective technology requires a high level of collaboration before, during, and after development. Successful coordinating agencies such as the DEA's Special Operations Division and the Air Force Enterprise Capability Collaboration Teams, along with many other joint task forces, deter stovepipe thinking that impedes progress. They also afford opportunities to improve and speed decision-making and the application of technology to meet requirements based on a holistic understanding of today's asymmetric battlespace.

This kind of holistic strategy for technology development involves interagency cooperation and private sector engagement. The goal is to optimize the entire nation's potential to apply diverse technological assets and operational concepts against asymmetric threats from cyber attack and espionage to global pandemics, as well as from nation state aggressors with nuclear capabilities or non-state actors.

History may provide a lesson on the challenges inherent in conceptualizing a third offset strategy. World War I was only labeled as such retroactively. At the time it was called "the war to end all wars." Similarly, in the 1950s, the nuclear offset strategy was not labeled the "first offset." It only gained this nomenclature by the necessity of a second, after the overwhelming superiority gained by nuclear capabilities proved insufficient to negate future conflicts.

Is the U.S. investing unwarranted confidence in the expectation that any technological advancement will be more than a strategic stopgap? There is no silver bullet, nor any technological advancement in which to load it, that is sophisticated enough to guarantee a lasting U.S. advantage. Whether the third offset is a set of technologies or a comprehensive strategy is also debatable.

What is the goal of the third, or any, offset strategy? Creating long-term, sustainable advantage is the generic answer. But advantage over whom? Unlike preceding countervailing strategies, the U.S. today faces significantly more diverse adversaries and complex threats. And with rapidly shifting goalposts, how will success be measured? The third offset must have a measure of success, while keeping in mind that there is no symmetry so conclusive as to guarantee the U.S. prevailing over future asymmetric threats.

ACKNOWLEDGEMENTS

Symposium Founders

Dr. J.P. (Jack) London
Executive Chairman and Chairman of the Board, and Former President and CEO, CACI International Inc

Dr. Warren Phillips
Professor Emeritus, University of Maryland; Board of Directors, CACI International Inc

Publisher and Editor-in-Chief

Dr. J.P. (Jack) London
Executive Chairman and Chairman of the Board, and Former President and CEO, CACI International Inc

Advisors

Ken Asbury
President and Chief Executive Officer, CACI International Inc

Jody Brown
Executive Vice President, Public Relations, Corporate Communications, and Congressional Relations, CACI International Inc

Michael Dolim
Executive Director, Association of Old Crows

Mike Gaffney
Executive Vice President, Business Development, CACI International Inc

Stephanie Giese
Vice President, Legal Division, CACI International Inc

David A. Hime
President, Association of Old Crows

Z. Selin Hur
Strategic Programs, Principal CACI International Inc

Ben Lerner
Vice President, Center for Security Policy

Dr. Warren Phillips
Professor Emeritus, University of Maryland; Board of Directors, CACI International Inc

Ron Schneider
Executive Vice President, Business Development, CACI International Inc

Symposium Participants
(in alphabetical order)

Lt Gen Robert J. "Bob" Elder Jr., USAF (Ret)
Professor, George Mason University

LTG Michael T. Flynn, USA (Ret)
Chairman and Chief Executive, Flynn Intel Group

Frank J. Gaffney
President, Center for Security Policy
Mr. Gaffney also served as Advisor

SES Mark Hamlet
Special Agent in Charge, Special Operations Division, Drug Enforcement Administration

Maj Gen Kenneth R. Israel, USAF (Ret)
Former President, Association of Old Crows
Maj Gen (Ret) Israel also served as Advisor

Dr. Lani Kass
Senior Vice President, Corporate Strategic Advisor, CACI International Inc
Dr. Kass also served as Advisor

Dr. J.P. (Jack) London
Executive Chairman and Chairman of the Board, and Former President and CEO, CACI International Inc
Dr. London also served as Advisor

Stephen Murphy
Special Agent in Charge (Ret)
Drug Enforcement Administration

Lt Gen Robert P. "Bob" Otto, USAF
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters, U.S. Air Force

Javier Peña
Special Agent in Charge (Ret)
Drug Enforcement Administration

Dr. John Shaw
Program Manager, Strategic Technology Office, Defense Advanced Research Projects Agency

Lt Gen Jack Weinstein, USAF
Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration, Headquarters, U.S. Air Force

Jody Westby, Esq.
Chief Executive Officer, Global Cyber Risk LLC

Jeff Wright
Consultant, CACI International Inc
Mr. Wright also served as Program Manager and Advisor

Dr. Greg L. Zacharias
Chief Scientist of the U.S. Air Force

Symposium Support Team

Event Manager

Erica Davis
Marketing Administrator, CACI International Inc

Participant Coordinator

Casey Pierce
Business Analyst, CACI International Inc

Report Lead

Ken E. Israel
Technical Writer, CACI International Inc

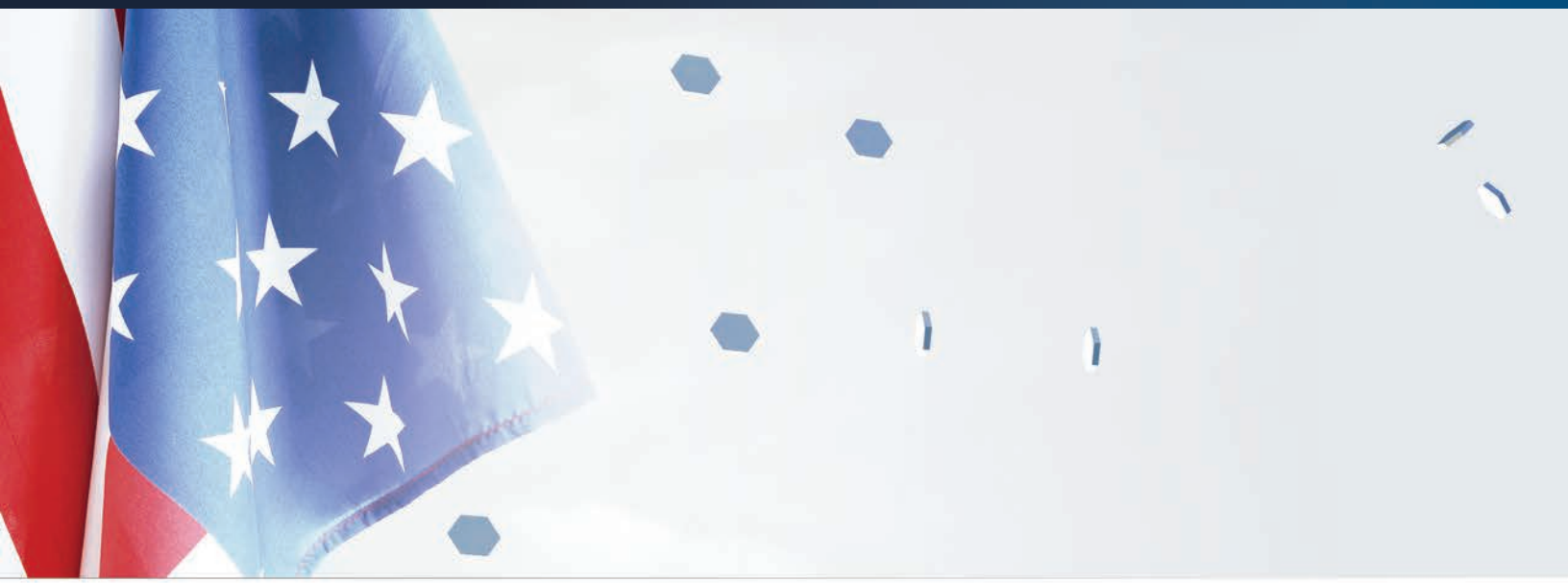
Editor

Michael Pino
Publications Principal, CACI International Inc

Art Direction and Graphic Design

Chris Impink
Lead Multimedia Designer, CACI International Inc

The Asymmetric Threat website **(asymmetricthreat.net)** serves as a knowledge network to advance the dialogue on national and global security, presenting resources and original research, and providing a forum for review and discussion of pertinent themes and events.



ASSOCIATION OF OLD CROWS

CENTER FOR SECURITY POLICY

CACI
EVER VIGILANT

Association of Old Crows
1000 North Payne Street, Suite 200
Alexandria, Virginia 22314-1652
(703) 549-1600
www.crows.org

Center for Security Policy
1901 Pennsylvania Avenue, NW, Suite 201
Washington, DC 20006
(202) 835-9077
www.centerforsecuritypolicy.org

CACI International Inc
1100 North Glebe Road
Arlington, Virginia 22201
(703) 841-7800
www.caci.com

asymmetricthreat.net