ASYMMETRIC THREAT
SYMPOSIUM XI

SOLUTIONS AND INNOVATIONS FOR DEFEATING ASYMMETRIC THREATS

COUNTERING ASYMMETRIC THREATS:
A NATIONAL IMPERATIVE

On October 17, 2018, at Valo Park in McLean, Virginia, CACI International Inc (CACI), the Center for Security Policy (CSP), the Institute for the Study of War, and the Mitchell Institute for Aerospace Studies co-sponsored the symposium, *Solutions and Innovations for Defeating Asymmetric Threats,* the 11th of the Asymmetric Threats to National Security series. The symposium series is designed to promote dialogue on critical national security issues, focusing on ideas, events, and technologies that drive the evolution of strategic thought and practice.

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 CACI, CSP, the Institute for the Study of War, the Mitchell Institute for Aerospace Studies, 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. Quotations within the document are non-attributed remarks from symposium participants.

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

The United States is facing a new warfare paradigm. The lethality, scale, scope, and velocity of potential conflicts have never been greater. Freedom – indeed, the American way of life – is at risk. Every domain – air, land, sea, space, and cyberspace – is now highly contested, due to the emergence of technologies that are changing the character of war. In order to deter adversaries and avert a global, high-stakes conflict, national security leaders need to fully harness America's technical ingenuity and talent and act with greater urgency to fine-tune and execute a multi-dimensional, holistic strategy. The 11th Asymmetric Threat Symposium, titled *Solutions and Innovations for Defeating Asymmetric Threats*, brought together leaders from the military, government, industry, and academia to discuss the current national security situation and examine ways to ensure the U.S. regains and sustains its competitive edge.

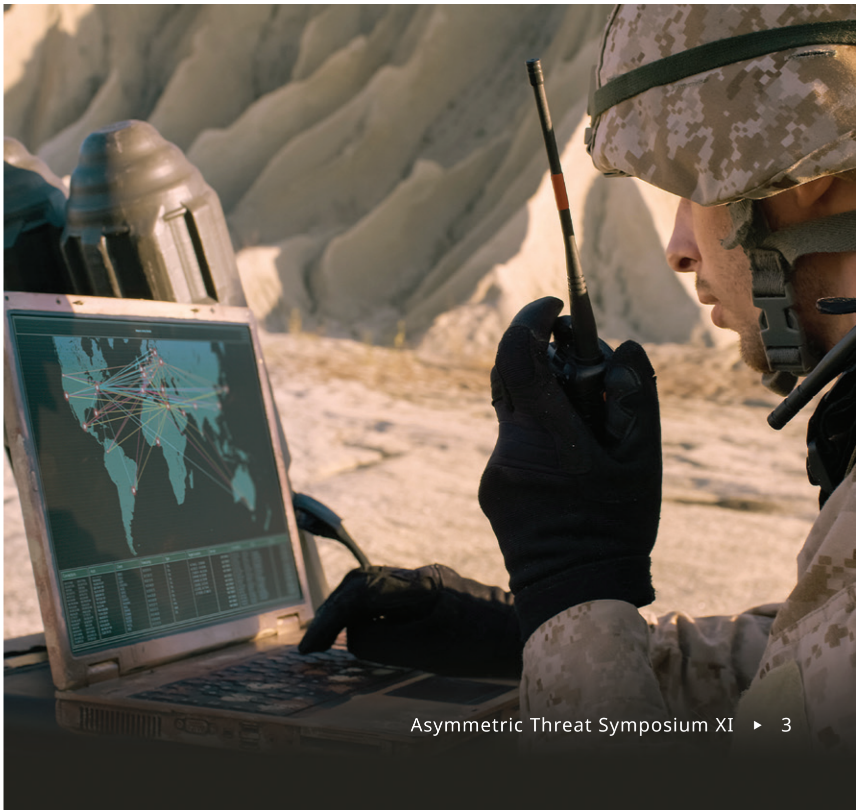
Seventeen years spent fighting terrorist groups at the lower end of the conflict spectrum have yielded technological and tactical breakthroughs, but have also taken a significant toll on U.S. troops and federal budgets without producing lasting outcomes. Throughout these years, adversaries – especially China and Russia – have benefited from studying U.S. military tactics, techniques, and procedures while observing a populace that seems to be increasingly disengaged from global affairs. These competitors developed technologies and approaches – all too often through cyber incursions and outright theft of U.S. government and industry secrets – aimed at undermining the global position of the U.S. and its allies. Without an adequate response that includes a substantial investment in countervailing strategies and technologies, these advances pose a dire threat to the U.S. and democratically elected governments everywhere.

The U.S. has been slow to adapt to a paradigm shift wherein its technological superiority can no longer be taken for granted, and control of the where, when, and how of warfare is no longer an exclusively U.S. prerogative. The U.S. must move quickly to define adequate policies and authorities that take into consideration both the moral and strategic implications of the new, diffused, diverse, and increasingly automated battlefield.

While the use of disinformation is as old as war itself, recent technological developments make it more difficult to determine the truth. Advances in electronic warfare and signals spoofing can render suspect the validity of imagery and even the locations of platforms and soldiers. Disinformation can now be amplified via the information ecosystem that includes social media and the Internet. Besides increasing doubt about whom or what to trust, disinformation campaigns polarize public opinion and decision-making, with instantaneous and far-reaching effects that can range from street protests to political upheaval and even civil war.

In such rapidly changing conditions, the U.S. cannot get by with current thinking and technologies. The key to future success is dynamic, sustained, and systemic innovation and readiness to take risk, as well as unwavering commitment and determination to prevail – all underpinned by sound, nimble, and timely decision-making.

▸ Adversaries have benefited from studying U.S. military technology in action.



1 The Changing Character of War

The U.S. cannot control when, where, and how military conflict begins. It can, however, prepare for the future by taking a fresh look at the very construct of war that is no longer confined by temporal, geographic, physical, or political boundaries. The methods and practices that led the nation to past victories are likely not those that will preserve peace and deter adversaries in the long run. Keys to prevailing in a highly dynamic global environment are innovation, agility, determination, and a great sense of urgency. It will require a new definition of risk because the greatest obstacle to success is that of stagnation: clinging to traditional methods and weaponry or doing the same old things with new tools.

"If we don't change, the margin is uncomfortably close, and the butcher's bill goes up."

The U.S. is slowly adapting to the new reality and the lack of clear delineation between peace and war. "Our campaigning is now through a continuum. We now talk about competition, short of armed conflict." Along this continuum, the military plays a supporting role to diplomacy and economic activity by deterring the competition from escalating into open hostilities. When diplomacy fails, the U.S. will have to determine what actions are worthy of military intervention. That decision will depend, in part, on the readiness and capabilities of the U.S. military and its allies, as well as the costs and risks of escalation in proportion to the value of the objective.

Although ideologically driven extremist groups continue to operate and proliferate across the Middle East, Asia, and Africa, it was the growing military strength and aggression of Russia and China that caused a significant shift in the U.S. National Defense Strategy. Other state actors, such as North Korea and Iran, remain under scrutiny, but the primary focus is on the grave, potentially existential, threats to U.S. national security interests posed by nuclear-armed Russia and China.

Both countries have built up their military capabilities to a level that is causing alarm. They have caught up to, and in many cases surpassed, the U.S. in the development and deployment of new technologies. They are eager to flaunt their new prowess and in doing so have already disrupted the international order, threatening the free flow of goods across the globe, the territorial integrity of neighboring countries, and the economic and political interests of the U.S.

Russia and China continue to show off their strength with provocative military actions that push – and in some cases trample – the boundaries of legitimacy, but are carefully calibrated to remain just under the threshold of military response. Such calculations are inherently dangerous, since Cold War red lines have become blurred. Russia has intercepted U.S. military planes flying over the Baltic and the Black Seas. It continues to threaten the Ukraine in several ways, including a military build-up on the Ukraine's eastern border and information campaigns to exacerbate tensions

▶ Chinese and Russian soldiers trained side-by-side during Russia's Vostok-2018 military exercises, their largest since the Cold War.

China's expanding territorial claims in the South China Sea overlap the UN-recognized waters and islands of several nearby nations.

among ethnic groups and inflame separatists on the western border. The Russian government has also been accused of using Internet troll farms to influence the Ukraine's 2019 elections and executing information campaigns that may be setting the stage for Russian military intervention in defense of pro-Russian separatists in the Ukraine. In November 2018, Russia tested international resolve by firing on and seizing three Ukrainian naval ships and 24 sailors in the Sea of Azov. The response included diplomatic condemnation by the U.S. and Europe, along with promises of financial assistance to the Ukraine, but the incident did not provoke military response from NATO allies or a U.N. Security Council resolution.

China is making strides in its own campaign to reset the international order in its favor. In its drive to control the region, China successfully militarized several natural and man-made reefs in the South China Sea and extended its territorial claims there. Where it once denied the military build-up, now China openly proclaims its “natural right” to deploy troops and equipment to bases on the islands, defying the territorial claims of the Philippines, Vietnam, and other neighboring nations. China has installed air bases there, along with anti-ship cruise missiles, surface-to-air missile systems, and electronic warfare equipment. It has sought to intimidate not only its neighbors but also the U.S. military. In one incident, a Chinese People's Liberation Army (PLA) naval vessel sailed within 45 yards of a U.S. guided missile destroyer in the disputed waters. Shortly afterward, two PLA Air Force jets nearly collided with a U.S. Navy reconnaissance plane.

These and other shows of military power appear to be designed to cause alarm in surrounding nations without provoking a direct confrontation with U.S. and allied forces. This type of aggressive behavior marks another milestone in the blurring of the lines between war and peace.

Less openly and without using lethal weaponry, China and Russia continue to attack U.S. government and industry networks. They probe weaknesses, map out connections, and pilfer both military and commercial intellectual property. The largest known cyber attack – although the perpetrator has not yet been named publicly – was the Yahoo attack of 2013, in which all three billion user accounts were compromised. Another significant attack was perpetrated on the Starwood Hotels Preferred Guest system. A Chinese intelligence group was blamed for this attack, which is said to have lasted from 2014-2018 and compromised the personal information of 500 million customers. In 2014, China was also blamed for the attack on the U.S. Office of Personnel Management that revealed the personal information of more than 20 million current and former government employees.

China has long targeted managed service providers (MSPs), who are responsible for monitoring the networks of multiple customers. Once the attackers breach an MSP, they have easy access to their customers. There is ample evidence of ongoing state-sponsored hacking into commercial databases of individuals and credit cards. The U.S. recently accused China of breaching several U.S. agencies, as well as the U.S. Navy personnel system, where cyber thieves stole the personal information of 100,000 personnel. This information is useful for espionage anytime and would be priceless in wartime.

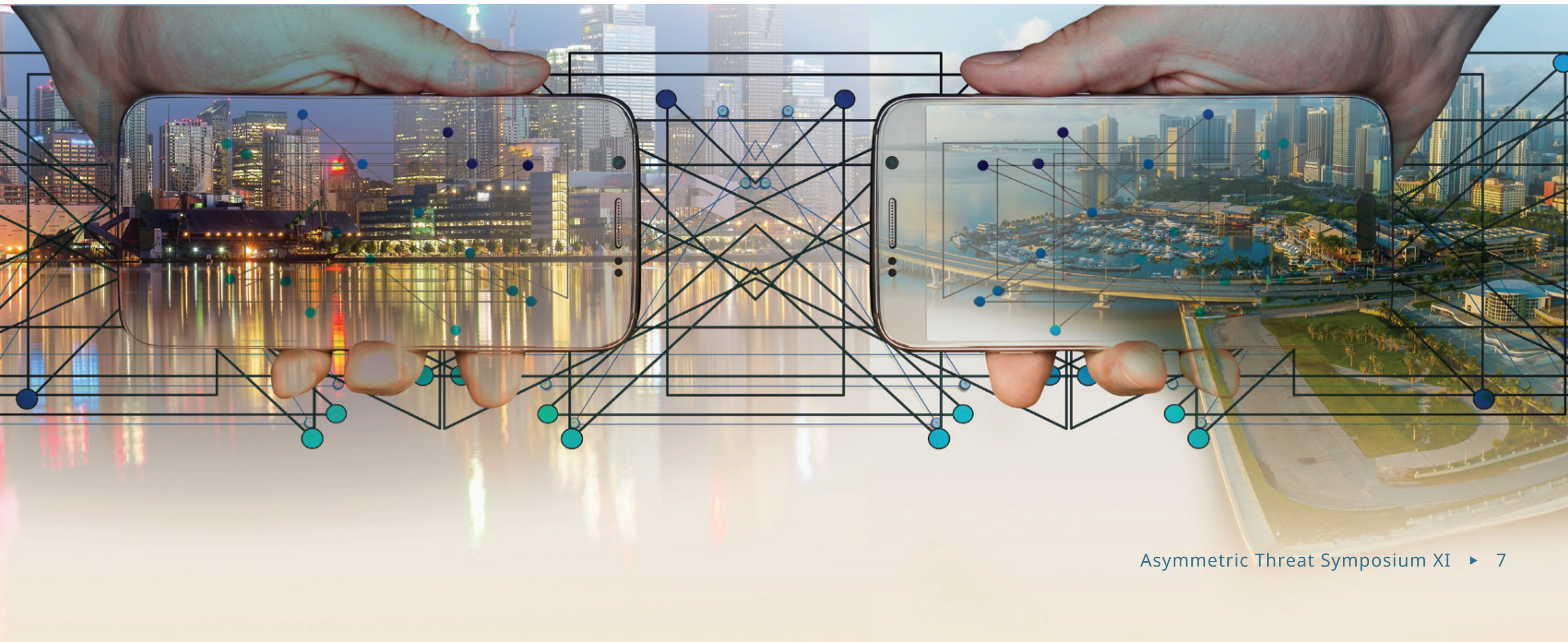
The Internet of Things Increases Vulnerabilities

The increased networking of military platforms and equipment, as well as the growing use of the Internet of Things in homes, industry, and government, is creating new vulnerabilities with few solutions. The systems were designed for ease of use, not security. Their light size does not allow much space for encryption. Worse, many manufacturers pay scant attention to security and have standardized passwords for their devices, leaving them wide open to attack. The Shodan website's search engine lists individual devices that have not changed the manufacturers' default passwords and even identifies their locations.

The vulnerability of military platforms extends into all domains, even space. Until recently, space was widely perceived as a conflict-free domain, open to international cooperation in pursuit of scientific advancement. The International Space Station, for example, continues to function despite a near total freeze in U.S.-Russia relations. When the U.S. Air Force developed and launched the first GPS satellites, the data was made free to people around the world, leading to great technological leaps that changed modern life. “Space is an integral part of our daily lives, our economic activity, our civilian infrastructure, the humanitarian activities we're involved in, weather, and position, navigation, and timing.” The data is used for everything from smartphone mapping and transportation applications to automated tellers and even fuel and food distribution systems.

China and Russia have long operated their own positioning, navigation, and timing (PNT) systems, but the U.S. military's use of satellites for communication and intelligence, surveillance, and reconnaissance during Desert Storm proved to be an asymmetric advantage that they could not ignore. Not surprisingly, they began to investigate ways to diminish American domination in space. In 2007, China test-launched an anti-satellite missile that hit its target, renewing earlier debate about the weaponization of space. As more countries and commercial entities launch and maintain PNT and commercial satellite constellations, finding ways to defend these satellites from interference is more urgent than ever.

Home and office devices are networked via simple protocols in the Internet of Things. The systems were designed for ease of use, not security, and are easy prey for hackers.



2 America's Eroding Technological Edge

The widespread use of the Internet, followed by the surge of smartphones, tablets, and other mobile devices, revolutionized the world economy. New technologies and services flattened competition and dethroned traditional leaders, upending almost every industry from retail and hospitality to transportation and health. Not surprisingly, the national security and defense industries have also felt the effects of the information revolution, which has diminished America's upper hand in global affairs. The ubiquitous availability of information has led to rapid advances in technology and sharp plunges in the costs of acquiring know-how and equipment. Services that were once the purview of a handful of wealthy nations are now as simple to acquire as logging into an app store on a smartphone. From securing communications and financial transactions to requesting satellite imagery and operating swarms of drones, any individual living anywhere on the globe now has access to a powerful array of tools and services that can be easily diverted for malign use. Neither large sums of money nor any special technological expertise is required.

"Could you have ever imagined a tribal militia capable of wielding advanced drone technology, firing precision anti-ship guided missiles and short range ballistic missiles?"

PNT Spoofing

All modern militaries have become heavily reliant on global PNT satellites and systems for everything from reconnaissance to laser-guided munitions. Ships, vehicles, and aircraft rely on the systems to navigate for both commercial and military purposes, but what happens when these systems fail? Or worse, when they are hacked and spoofed, leading vessels, vehicles, and people to believe they are in a location that is actually miles away from their objective?

The modern economy is reliant on positioning, navigation, and timing systems. What happens when they are spoofed?

Image courtesy of NASA

GPS spoofing has been around for a while, but the popularity of the online "Pokemon Go" game pushed it into the mainstream. After all, why travel great distances to gain points in the game, if you can simply spoof your phone into thinking it is already there? Inexpensive commercial spoofing applications followed shortly after the game debuted and can now be easily downloaded onto any smartphone.

The first publicized large-scale GPS spoofing incident occurred near the Russian port of Novorossiysk in the Black Sea during the summer of 2017. More than 20 vessels reported a "glitch" in their PNT systems that showed their location to be 32 km inland from their true position, placing them near an airport. GPS systems near the Kremlin are also said to send out false information, and there have been ongoing reports of GPS systems placing vehicles and vessels near Russian airports. The reason for this spoofing seems to be drone deterrence near sensitive targets, such as government installations and even President Vladimir Putin's Black Sea residence.

The military applications of spoofing are clear – if PNT systems on ships, aircraft, and tanks can be misled, it follows that their guided munitions could be fooled into thinking they are hitting a target far away from the original objective. Another risk is that imagery satellites could relay information that appears to show one location, when the action is really happening in another.

Even when spoofing is not involved, the ability of ships to turn off their navigation systems and "go dark" poses a risk. Thousands of vessels "went dark" while entering European waters after turning off their PNT systems last year. Many are likely involved in drug smuggling and human trafficking. More ominously, several of the ships navigated close to countries such as Libya and Syria prior to going dark, suggesting possible involvement in terrorism. Besides the likelihood that they are masking illicit activities, vessels that go dark put all the other sea traffic in danger of collision. Now that driverless vehicles and delivery drones are well on the path to commercialization, their reliance on GPS and artificial intelligence magnifies the risk on land and in the skies.

GPS systems on radio-controlled autonomous aircraft have allowed them to be weaponized in ways that were unforeseen just a few years ago. The Islamic State pioneered the use of these inexpensive, commercial hobby drones for

The Day Nuclear War Was Averted

On September 26, 1983, the Soviet Union's nuclear early-warning system signaled an incoming attack by a U.S. ballistic missile. Lieutenant Colonel Stanislav Petrov was the duty officer at the Soviet Air Defense Forces command center that night. According to protocol, he was expected to advise his superiors immediately so they could prepare a massive counterattack to prevent the U.S. from destroying Soviet launch sites.

Petrov initially dismissed the signal, reasoning that a full-scale attack by the U.S. would involve dozens, if not hundreds, of missiles. Shortly thereafter, the system signaled that four more missiles had been launched from the U.S. Sirens wailed. Every second wasted meant less time for a Soviet response. Still he waited.

When he finally picked up the phone, Petrov reported a system malfunction – not the start of a nuclear war. He was, obviously, correct. A rare alignment between Russian satellites and sunlight on high-altitude clouds had generated the false signal. His experience, courage, and reasoning prevented a nuclear catastrophe.

What happens if such decisions are relegated to machines?

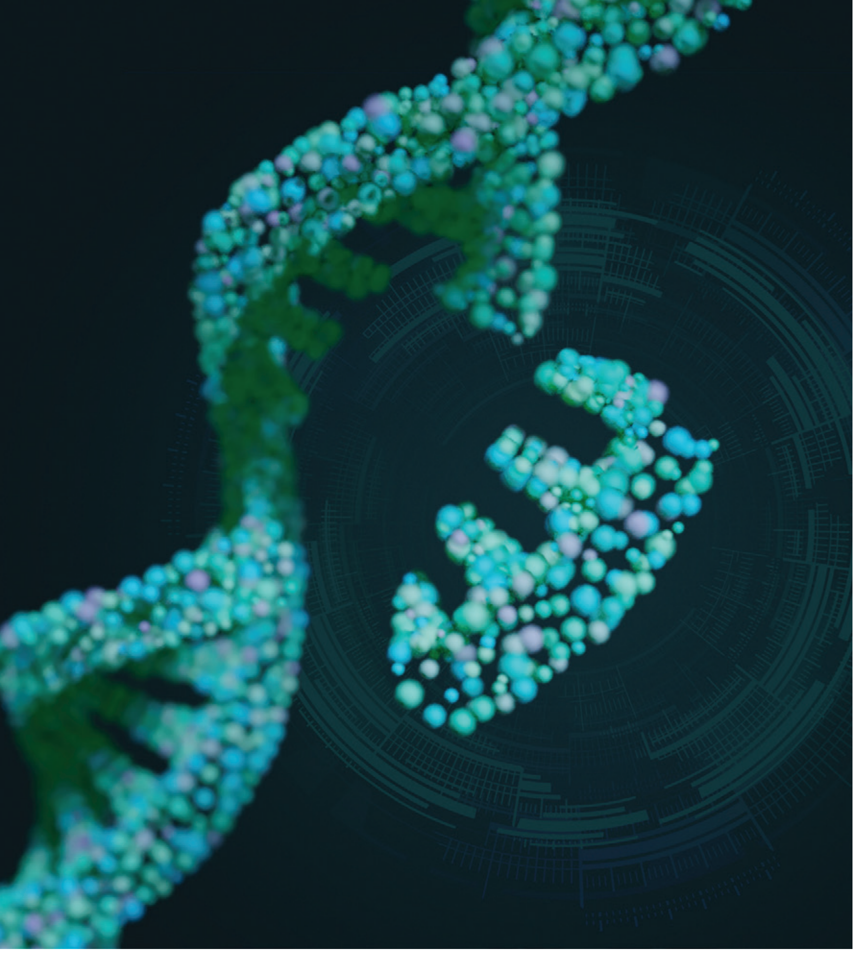
▸ Inroads in artificial intelligence applications make ascertaining the veracity of audio and video a challenge.

reconnaissance, deception, and strike purposes, loading them with grenades and attacking U.S. and coalition forces. They developed and filmed bomb-making workshops to weaponize drones, some of which can carry a payload of up to 40 kg. Quadcopter drones are readily available and can reach speeds of close to 200 mph. The 2016 Guinness world record for a radio-controlled turbine jet was 462 mph. The event was captured on YouTube and garnered more than 3.5 million views. "The speed and agility of these platforms are starting to exceed the neurologic response capability of the human brain." Since the operator has now become the limiting factor, competitors – and, most likely, terrorists – are studying how to apply artificial intelligence to drones: "We don't have a solution for this. We've got to find one."

Another challenge is the recent development of GPS precision-guided handheld firearms – they are easy to use and 70-80 percent accurate. Whereas a top-level sniper requires many years of practice and experience, training young soldiers to use precision-guided weaponry is far easier and has the potential to yield significant savings for the U.S. military. The problem is that adversaries can use the same technology, giving them skills that would otherwise take years to develop.

What Can You Trust?

Artificial intelligence applications now include search engines, language translators, and voice-activated applications, such as Siri® and Alexa®. They are being used to help solve a vast array of tasks in industry and government. However, these advances are also exploited to confuse and deceive. New video applications allow faces to be superimposed on other bodies and can mimic the behavior of specific human targets. Soundtracks are easily spliced and edited, and even voice prints can be altered in real time. All of this makes ascertaining the veracity of videos and telephone conversations problematic, with implications for many fields, including military, intelligence, law enforcement, and politics.



Easy access to DNA manipulation technology increases the risk of biological warfare.

DNA Manipulation

The spread of information and computerization has also caused the costs of biotechnology to plummet. What used to require very high levels of expertise is now available to the public. One headline-grabbing example is the giant leap forward in DNA manipulation and gene editing brought about by Clustered Regularly Interspaced Palindromic Repeats (CRISPR) Cas-9. This engineered enzyme locates genetic sequences and can cut DNA apart. In the few years since its introduction, CRISPR Cas-9 has upended the biotechnology industry and has already been used to develop climate-resilient crops, treat genetic diseases, and even sterilize mosquitoes. Its adoption caused grave ethical concerns when a Chinese scientist announced he used it to create a pair of gene-edited human babies.

For the national security community, the ease of access to DNA manipulation technologies means the creation of sophisticated bioweaponry will no longer be limited to advanced peer competitors. Learning the basics of gene manipulation can now be done by ordering low-cost kits online and watching videos on YouTube. The concern is that legally or morally unrestrained individuals and groups have access to technologies that could be used for bioweapons. Even those who intend no harm but are untrained in proper laboratory procedures could unintentionally release biologically manipulated organisms into the ecosystem with unforeseeable repercussions.

Blockchain

Like most leaps in technology, the advent of blockchain technology is filled with promise and peril. Blockchain relies on a vast, decentralized, globally distributed network of computers

Digital currencies like BitCoin are based on blockchain, an encrypted distributed ledger system. Criminal groups use the technology to avoid detection of their activities.

with a shared database. The computers in the network continually reconcile and validate transactions that are associated with a certain date and time. These encrypted transactions cannot be interfered with by outsiders, because any change to the data is visible to the entire network. This enables what amounts to a digital "handshake" between parties who often remain anonymous. The resulting information integrity enables so-called "smart contracts" and improves tracking of supplies and equipment. However, it also poses a challenge to national security.

Blockchain is the underlying technology of digital currencies. It was originally invented as the public ledger for BitCoin digital currency. Digital currencies currently number over 1600 and several are accepted by legitimate businesses – the state of Ohio even accepts BitCoin for tax payments – but they are also being used by criminals to buy and sell everything from drugs to weapons to humans. Counterterrorism and homeland security experts have long tracked illicit groups via their financial transactions, but with blockchain, the ability to "follow the money" is greatly diminished.

Encryption itself has become more prevalent, with common applications often featuring very advanced encryption. "The next time you're trying to download some app, note the number of apps that offer 256-bit or stronger encryption, which in many cases, nobody can break. If that's not an asymmetric problem, I don't know what is."

The Weaponizing of Social Media

The attempt to expand influence, affect public opinion, and undermine adversary governments is as old as war itself.

"What's different is that technological advances – social media platforms, the degree to which false email accounts and various identifiers can be created – now allow those individual operations at scale, and it's far, far harder to determine which entities are involved."

Social media platforms, especially Twitter and Facebook, have been under fire for not doing enough to recognize and remove accounts of false personas. Are the platforms accountable for the content published by their customers, when one of their stated purposes is to level the media playing field and give everyone an equal voice? How can they remove suspicious accounts without stepping on the rights of individuals to freedom of expression?

3 Solutions and Innovations

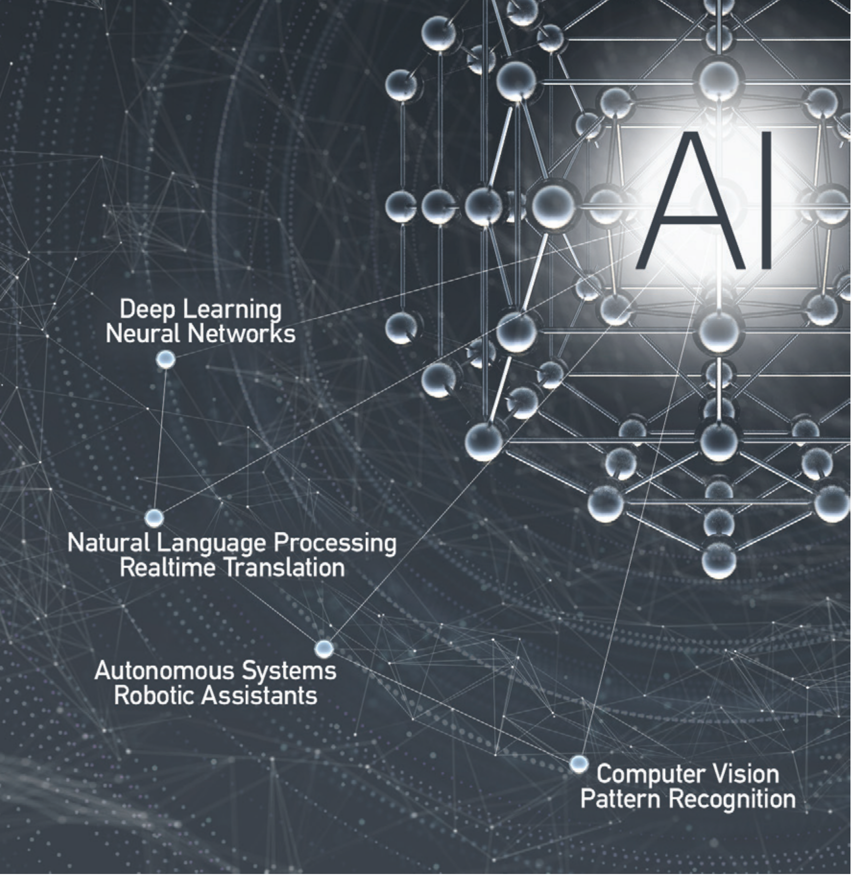
The complexity of the threat environment faced by the U.S., as well as the velocity at which new threats arise, suggests that no simple response will be forthcoming. What seems clear is the need for innovation in every dimension of the national security environment, backed by an openness to listen, learn, and encourage change at a rate that is certain to cause discomfort. This will require educating more junior leaders to understand their commanders' intent, assume more initiative and risk, and think on their feet using technology as an aid for split-second decision-making. Good ideas have no rank, and senior leaders must both listen to their subordinates and empower them to act independently within broad, flexible guidance. Leaders at all levels must have in-depth knowledge of the capabilities and motivating forces of adversaries. They must have a collaborative mindset to accomplish joint, multi-domain warfare. This will require high levels of trust in, and knowledge of, each others' capabilities and limitations. Information sharing across the Services, the Interagency, and alliances is also key. The good news is that these changes are underway, but progress must be accelerated because adversaries are fast approaching – and in many cases surpassing – the U.S. with new capabilities and new uses of technology.

"I think the area where we are lagging most, and our opponents are gaining the most ground, is the ability to imagine and the speed at which they can turn imagination into reality."

Innovation is, as it always has been, key to maintaining an asymmetric edge. The speed at which technology changes and is adopted means the U.S. must become extraordinarily nimble. The spirit – indeed the imperative – of innovation must permeate the national security community, not only in terms of adopting new technologies, but across the board: from how military and intelligence personnel are educated and trained throughout their careers, to how individuals are promoted and recognized, to how operations are executed and concluded. It is essential to enable collaboration among "digital natives," such as scientists, engineers, and military and intelligence professionals. Such cooperation is necessary for the development and adaptation of novel technologies – as well as tactics, techniques, and procedures – to compete, fight, and win across the conflict spectrum. It is equally essential to avoid the trap of using new technologies in old ways.

To avoid overreliance on PNT systems, cadets at military academies and in ROTC courses are once again learning to navigate by the stars, read paper maps and charts, and use sextants and compasses.

The U.S.'s ability to work closely across commands and Services, as well as with allies and coalition partners, remains a powerful asymmetric advantage. The military is adapting to a new paradigm of multi-domain, globally integrated warfare, where absolute superiority in all domains is not always required, but speed and back-up capabilities are. Even with resilience factored in, the truth is that no domain is impermeable. Thus, cross-domain dominance – the ability to compensate for disadvantage in one domain through superiority in another – and system redundancy become crucial.



Artificial intelligence has broad applications throughout the national security mission set. It can be used to speed and improve decision-making.

To avoid overreliance on PNT systems, for the first time in more than a decade, cadets at military academies and ROTC courses are learning to navigate by the stars, read paper maps and charts, and use sextants and compasses. These "old-fashioned" techniques require more math skills than today's technologies. Command, control, and communications are being reevaluated as well: "As a global operating force, the best way is to rely on space-based communications, but as military planners, we should be looking at multiple communications. We ought to ensure we have an airborne layer, a terrestrial layer ... In some cases, you ought to plan all the way down to the hand signals you're going to use."

In this new paradigm of multi-domain and "gray-zone" warfare, the value of allies cannot be understated — not only for their military capabilities, but also for their ability to add diplomatic and economic weight. Unilateral sanctions cannot work in an inter-connected world. Likewise, no single country can face and defend against the seemingly endless array of adversaries and malicious actors. In recent wars, information sharing among allies has proven to be an indispensable advantage. The U.S. and its allies must also be thoughtful in developing complementary capabilities to spread costs and ensure the highest performing technology is adopted and made interoperable.

Among U.S. Military Services, geographical divisions also need to be reconsidered, as adversaries – especially in space and cyberspace – are not limited by geography. Collaboration and information sharing are essential. The creation of a dedicated Space Force Combatant Command will bolster the military's ability to respond to emerging threats in the space domain, as will the sharing of capabilities among key allies via the the Combined Space Operations Center. Regardless of domain, "Every process, every aspect of strategy must be seen from the perspective of globally integrated operations."

Another area that requires attention is the notoriously cumbersome and lengthy federal acquisition process. It has often delayed testing and fielding of new technologies, although recent changes promise to make the process more adaptive to emerging needs. Government customers with time-sensitive requirements are beginning to adopt new acquisition vehicles that enable faster research, development, testing, and fielding of advanced equipment. Agile development and readiness to accept and learn from failures are equally important.

With a plethora of tasks and inherently limited funding, national security leaders are now looking for lower-cost solutions wherever possible. "We too often find ourselves on the wrong side of the cost curve, where our systems become a target that is significantly more sophisticated and expensive and harder to replace than the round." The reverse is also true: highly sophisticated weapons used against low-value targets place the U.S. on the wrong side of the cost imposition curve. The Islamic State revolutionized the use of low-cost, widely available unmanned systems to deliver explosives. To remain competitive, the U.S. should likewise strive to leverage and adapt inexpensive, commercially available technologies to military purposes.

Controlling the costs of developing and adopting new technology is essential. As the national security community invests in new capabilities, the entire lifecycle cost of hardware and software – as well as user training – must be taken into account. Fielding user-centric devices that require minimal training is essential, because the costs of training the operators and sustaining the system often exceeds the original price.

The Intelligence Community and the military are implementing several programs that use artificial intelligence (AI) to lower costs, improve decision-making, and reduce response time. AI has been especially useful in performing repetitive, routine tasks, saving hours of labor and freeing human operators to work on more strategically complex and ethically challenging problems.

Artificial intelligence and machine learning have broad applications in every domain. AI is essential to the deployment of autonomous vehicles, aircraft, sea vessels, submarines, and satellites. It allows the performance of risky tasks without endangering human lives. With millions of cubic miles in the space domain, machine learning can help protect U.S. assets more efficiently than previously possible. Algorithms can also be used to detect, identify, and track electronic signals and other sources of intelligence. AI contributes to the monitoring of vast computer networks by performing access control, identifying software applications, and discovering and responding to unwanted activity. New facial recognition software allows faster identification and better surveillance of targets. For now, all decisions involving lethal measures are left to humans. However, the U.S. must contend with the prospect that adversaries might be less morally and ethically constrained – especially as decision speed becomes the critical factor in the equation.

Spurred by peer-state adversaries, the U.S. is focused on an array of cutting-edge technologies. Both China and Russia have developed and tested hypersonic missiles. The U.S. must devise both a robust missile defense and new offensive capabilities. Hypersonic aircraft – which fly at six times the speed of sound – will enable the U.S. military to respond faster from greater distances, reducing reliance on forward-basing and projecting power without projecting vulnerability. The U.S. is also investing in quantum computing, directed-energy weapons, miniaturized “swarm attack” drone technologies, and special materials. These and other technological advances will undoubtedly shape future military engagements, but modernizing the nuclear triad and the C3 system that underpins it remains an essential and urgent priority. The military might of the U.S. and its allies must be sufficient to deter conflict, especially global conflict with peer-states, and should deterrence fail – to fight and win.

During training flights, Russia has successfully launched hypersonic Kinzhal missiles from MiG-31 fighter jets such as this.

Image courtesy of kremlin.ru

4 Conclusions

Modernizing tools, technologies, and conceptual approaches is essential for America to maintain peace, deter conflict, and prevail in war. Complacency is the path to peril, and incremental steps are equally dangerous. The key to future success is dynamic innovation – intense, sustained, systemic – that encompasses technology, organizations, and strategic concepts at the speed of need.

Most of all, innovation is required in thought and perspective, as well as in the ability to anticipate – to conceive, define, and quickly implement – high-value solutions ahead of adversaries. To this end, it is essential that frequent, purposeful communication take place at all echelons of the Services and industry, among multi-disciplinary scientists, engineers and cyber experts in all domains: Soldiers, Sailors, Airmen, Marines, and Cyber and Space Operators. Insight is gained through understanding of and trust in each other's expertise and experience, combined with deep knowledge of available technologies and a healthy dose of imagination and daring.

Multi-domain operations are the future of warfare, requiring full integration of electronic and cyber warfare into battle planning at all levels. Resiliency and redundancy must be built into all aspects of the national enterprise – especially command and control – such that an attack on one system or domain cannot cripple the others. Likewise, the U.S. must maintain a credible deterrence posture, predicated on demonstrated capability and will. Adversaries must understand that the cost of retribution would far exceed any potential gain from aggressive behavior.

It is also essential to involve the American public and leaders. From elected officials and diplomats, to the intelligence and military communities, and throughout government and industry, Americans must be aware of the real and present dangers the U.S. faces. The very freedoms that citizens hold dear – and, often, take for granted – are at stake. Only with determination and unity of purpose – accompanied by a keen and unwavering spirit of innovation – can America deter and prevail.

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 R. 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, Communications, CACI International Inc

Lieutenant General David A. Deptula, USAF (Ret)
Dean, Mitchell Institute for Aerospace Studies

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

Stephanie Giese
Vice President, Legal Division, CACI International Inc

Z. Selin Hur
Strategic Programs, Principal, CACI International Inc

Dr. Kimberly E. Kagan
President, Institute for the Study of War

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

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

Maseh Zarif
Director of External Relations, Institute for the Study of War

Symposium Speakers and Panelists (in order of appearance)

Jeff Wright
Consultant, CACI International Inc

Mr. Wright also served as Program Manager and 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

Lieutenant General Daniel J. O'Donohue, USMC
Director for Joint Force Development (J7), Joint Staff

Anne Neuberger, NSA
Senior Advisor to the Director, National Security Agency; NSA Lead, NSA/USCYBERCOM (USCC) Election Security Small Group, NSA

Lieutenant General Bruce A. Wright, USAF (Ret)
Senior Fellow at the Mitchell Institute for Aerospace Studies

Lieutenant General David D. Thompson, USAF
Vice Commander, Air Force Space Command

Lieutenant General Michael K. Nagata, USA
Director of Strategic Operational Planning, National Counterterrorism Center

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

Dr. Kass also served as Advisor

VADM Lowell (Jake) Jacoby, USN (Ret)
Jacoby Associates, LLC

Frank J. Gaffney
President, Center for Security Policy

Mr. Gaffney also served as Advisor

Cathy Lanier
Senior Vice President, Chief Security Officer National Football League (NFL)

Symposium Support Team

Report Lead

Tricia Branagan
Strategic Communications Lead, CACI International Inc

Art Direction and Graphic Design

Chris Impink
Lead Multimedia Designer, CACI International Inc

Event Manager

Erica Davis
Marketing Administrator, CACI International Inc

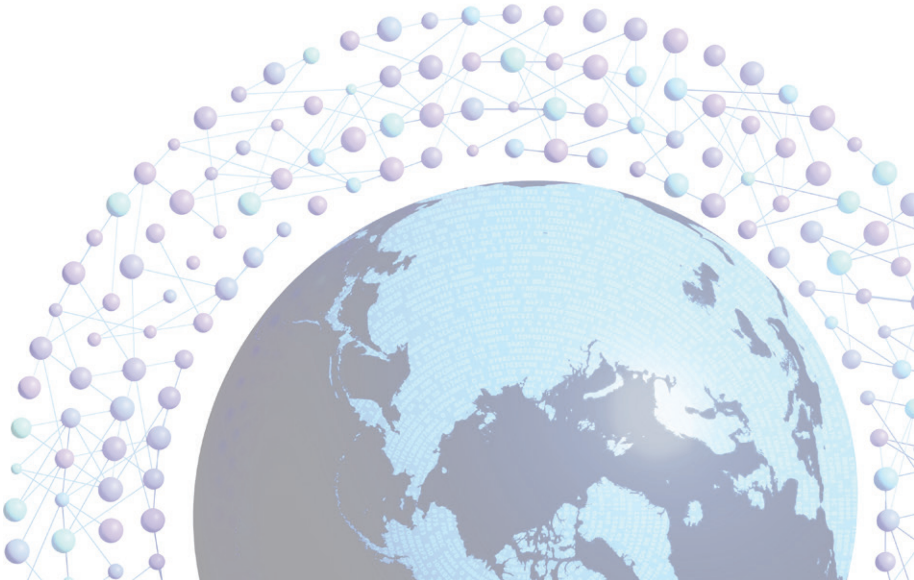
Editors

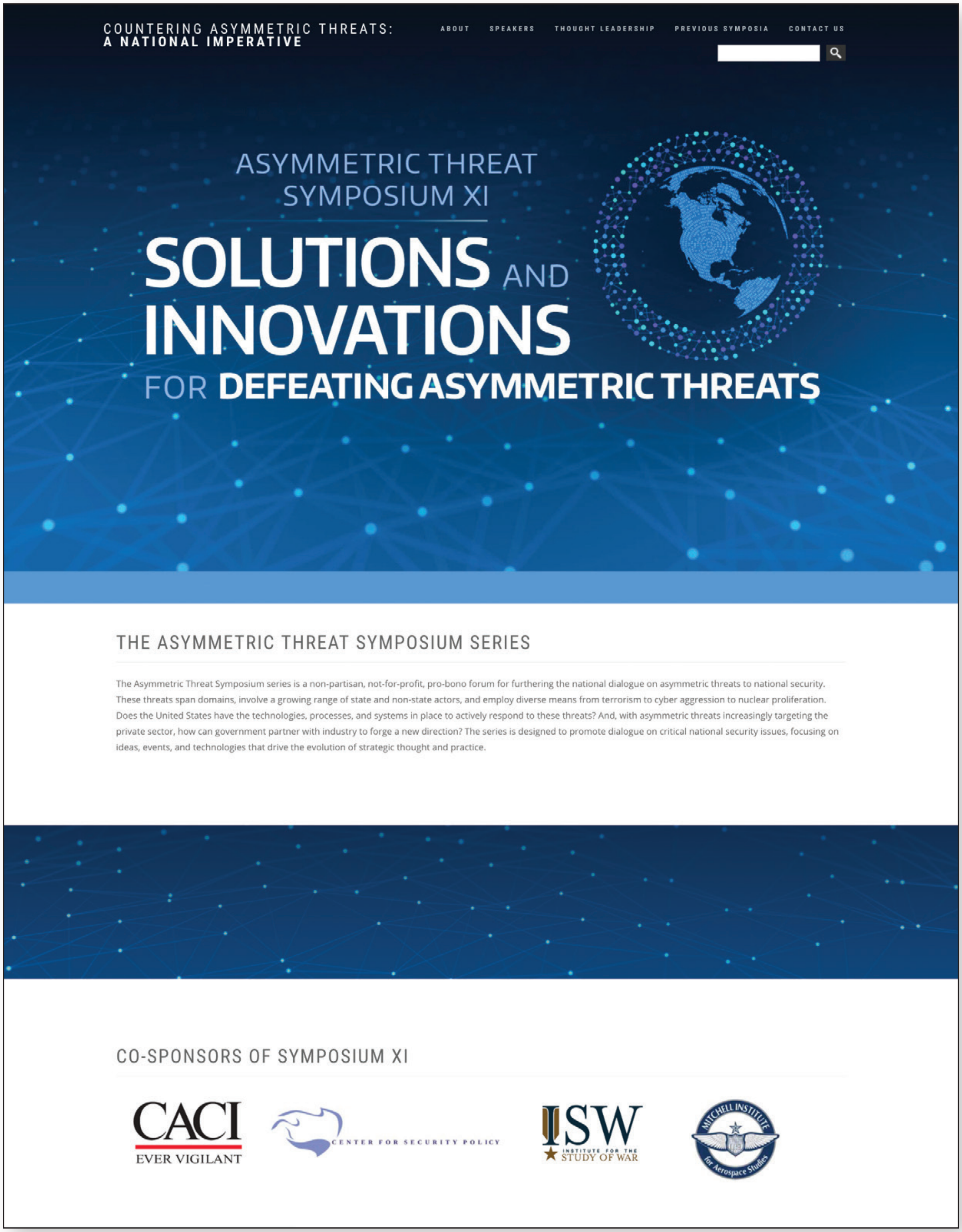
Erika Glon
Director, Marketing, CACI International Inc

Michael Pino
Publications Principal, CACI International Inc

Participant Coordinator

Casey Pierce
Business Analyst, CACI International Inc





THE ASYMMETRIC THREAT SYMPOSIUM SERIES

The Asymmetric Threat Symposium series is a non-partisan, not-for-profit, pro-bono forum for furthering the national dialogue on asymmetric threats to national security. These threats span domains, involve a growing range of state and non-state actors, and employ diverse means from terrorism to cyber aggression to nuclear proliferation. Does the United States have the technologies, processes, and systems in place to actively respond to these threats? And, with asymmetric threats increasingly targeting the private sector, how can government partner with industry to forge a new direction? The series is designed to promote dialogue on critical national security issues, focusing on ideas, events, and technologies that drive the evolution of strategic thought and practice.

CO-SPONSORS OF SYMPOSIUM XI

CACI
EVER VIGILANT
CENTER FOR SECURITY POLICY
ISW
INSTITUTE FOR THE STUDY OF WAR
MITCHELL INSTITUTE for Aerospace Studies

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.

CO-SPONSORS

CACI
EVER VIGILANT

CENTER FOR SECURITY POLICY

ISW
INSTITUTE FOR THE
STUDY OF WAR

MITCHELL INSTITUTE
for Aerospace Studies

asymmetricthreat.net

Sponsorship does not imply endorsement by the Department of Defense or any other agency or department of the U.S. Federal Government.