WHAT DOES IT TAKE TO PROTECT AMERICA?

Combatting Global Asymmetric Threats

10th ASYMMETRIC THREAT SYMPOSIUM

★ 2008 · 2017 ★

Countering Asymmetric Threats:
A National Imperative

On October 26, 2017, 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, *What Does It Take to Protect America? Combatting Global Asymmetric Threats,* the 10th 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

ASYMMETRIC THREAT SYMPOSIUM X

WHAT DOES IT TAKE TO PROTECT AMERICA?

COMBATTING GLOBAL ASYMMETRIC THREATS

The United States faces a broad, diverse, and increasingly complex array of threats, emanating from ambitious peer competitors, rogue nation-states, and non-state actors. Amidst this global uncertainty, the U.S. declaratory policy and core missions remain fundamentally unchanged: reassure allies, deter adversaries and, if deterrence fails, fight and win decisively in any contingency.

Is this posture credible, sustainable, and sufficient? What changes – in policies, authorities, technologies, and strategic approaches – are required to better safeguard America's global interests and prevail against the ever-expanding spectrum of threats? The 10th Asymmetric Threat Symposium, titled *What Does It Take to Protect America? Combatting Asymmetric Threats,* brought together leaders from a cross-section of military, government, industry, and academia to address these questions, providing insight and considerations to help chart the way forward.

In such a complex operating environment, and with adversaries so diverse, it has become clear that the U.S. must do new things in new ways or fall behind. America's technological, strategic, and operational edge has eroded after more than a decade of fighting at the lower end of the conflict spectrum. Meanwhile, adversaries have studied the events carefully and made significant technological and tactical progress. In addition, they have increasingly targeted U.S. citizens, institutions, and democracy with sophisticated, pervasive information operations and information warfare. Consequently, the U.S. faces an environment where every domain – land, sea, air, space, and cyberspace – is congested, contested, and potentially denied.

America's nuclear triad – the ultimate asymmetric advantage – is aging rapidly. The anticipated costs of modernization and recapitalization are staggering, yet the proliferation of nuclear weapons and the means to deliver them necessitates both new systems and new deterrence concepts, suitable to the rapidly evolving, asymmetric, multipolar world. Operational concepts, innovative technologies, and improved tactics, techniques, and procedures all must be delivered at unprecedented speed.

In this increasingly inhospitable environment, human factors – an area of traditional U.S. advantage – gain an even greater weight. This places a premium on recruiting, training, and retaining the future force. Novel approaches must incorporate new technologies and decision-making paradigms – including human-machine teaming – while at the same time enabling operators to move with only broad guidance in complex conditions that require a finely tuned moral compass and the readiness to take risk.

Time is not on America's side, but one thing is certain: "It's everybody's job to protect the country." The American people must be made better aware of the dangers and the required responses. The ability to harness the nation's talent, ingenuity, will, and determination is – as it has always been – the key to victory.

More than 70 years after the bombings of Hiroshima and Nagasaki, the threat of nuclear devastation remains the most effective deterrent to war between major powers.

1 The Spectrum of Asymmetric Threats

The core question embedded in the symposium's title, *What Does It Take to Protect America? Combatting Global Asymmetric Threats,* reflects the realization that the world is at an historic inflection point, wherein a combination of technological, political, social, economic, and cultural factors changes all the answers – as well as many of the questions. This inflection point portrays a complex threat array, featuring peer-state adversaries and competitors; foreign and domestic terrorism; and a volatile, rapidly changing, and increasingly hostile global environment. The historically bright line between peace and war has been blurred, raising the question whether the U.S. is already engaged in a multi-front conflict but hasn't yet fully grasped that reality – or responded accordingly. Dealing with these challenges requires clarity of vision, savvy engagement, and uncommon agility – particularly given that the U.S. simply cannot be physically present everywhere or do everything simultaneously.

"The volume of threat is absolutely unprecedented. The breadth of the threat is enough to stretch anyone's brain." While these threats are not limited to specific countries, the U.S. is focused on key state and non-state actors, each with its own unique history, strategy, and goals. Peer-state competitors China and Russia are challenging the U.S. with advancements across all five domains: land, sea, air, space, and cyberspace. Their rogue state neighbor North Korea has made great progress with its nuclear pursuit, and rattled its neighbors with every new missile test. Iran stirs political discord and arms rebel groups throughout the Middle East. The country insists its nuclear program is strictly peaceful, but the threat of its potential to precipitate nuclear escalation cannot be ignored. Ruthless terrorist groups such as the Islamic State continue to inspire followers despite their defeats on the battlefield. In addition, the U.S. continues to be targeted with sophisticated information operations by several different sources. Understanding how to best defend against such a broad range of threats requires a united effort that leverages every component of the U.S. national defense and diplomatic community, as well as those of allies and coalition partners.

"The volume of threat is absolutely unprecedented. The breadth of the threat is enough to stretch anyone's brain."

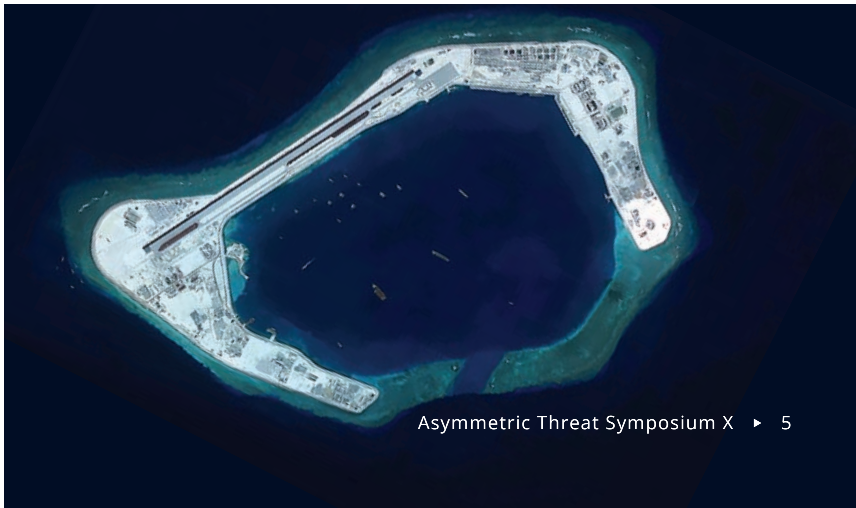
China

Fueled by its economic success over the past few decades, China continues to make significant investments in highly advanced technologies with military applications. From artificial intelligence and hypersonic vehicles to directed energy and cyberwarfare, China is making rapid progress with no signs of slowing down. Having mastered the art of committing hostile actions – both covert and overt – that remain just under the threshold of military response, China poses a threat to the stability of Asia and to the U.S. as the preeminent Pacific power.

The most glaring example of this is the build-up and militarization of artificial islands in the South China Sea. China managed to construct bunkers and landing strips, and deploy fighter aircraft and anti-ship and air defense missiles to the islands – effectively expanding its defense perimeter – without provoking a

The Chinese built naval facilities on Subi Reef in the Spratly Islands.

Imagery ©2018 Data SIO, NOAA, U.S. Navy, NGA, GEBCO, DigitalGlobe
Map data ©2018 Google



China’s Smart Big Brother App

An eye-opening example of the Chinese government’s enormous power is an all-in-one application for smart phones, known as the WeChat app. From Internet navigation, voicemail, and messaging to email, photos, digital wallet payments, and mapping, the application grants Chinese citizens the ease of modern living with a catch. WeChat is owned by a private company, Tencent, but heavily supported by the government. Thanks to China’s extensive monitoring and censorship, which includes all the WeChat servers, the app is effectively supplying the Chinese government with staggering amounts of information about more than 900 million citizen users and their everyday lives and habits. WeChat is now poised to issue officially sanctioned virtual ID cards to be used in lieu of state-issued ID cards. Also coming soon is an official citizen “trust” score. It will be based on the individual’s spending habits, social media use, and even friendships. That trust score will be used to determine permission to travel, as well as access to schools, mortgages, and jobs.

military response from its neighbors or the U.S. Its success has disrupted the equilibrium of the Pacific area and seems likely to lead to further upheaval, as Pacific Rim nations seek accommodation or protection.

China also presses on with its cyber espionage program, hacking U.S. technology companies, government, and military institutions. The hackers seem to have mapped out much of the U.S. infrastructure and have stolen intellectual property on a grand scale, allowing China to save significant amounts of time and money in the development of advanced technologies and weaponry.

With government control of the Internet, Chinese leaders seek to shield citizens from outside influences, and track almost every move they make, along with every message they post. The Chinese have developed and implemented government-controlled knock-offs of American technology and social media applications – unburdened by the time and capital that U.S. entrepreneurs invested to create and hone these industry-disruptive innovations.

> “China sends 300,000 students to U.S. universities each year, almost all of whom study STEM subjects.”

China’s focus on technology extends to education: its universities graduate approximately eight times the number of science, technology, engineering, and math (STEM) majors as the U.S. does. China also sends 300,000 students to U.S. universities each year, almost all of whom study STEM subjects, often at the Ph.D. level or higher. This risk of technology transfer may include a silver lining, as these same students experience a degree of freedom they have probably never imagined. “China is betting that they can take home 300,000 America-educated engineers and use that as a national power. I think it is just as likely that these young people will go back with Western values, and that is a threat to China. Sooner or later, they may actually be a little concerned about it.”

Russia

Like the Chinese, the Russian government skillfully calibrates its aggressions to a level that avoids direct U.S. and NATO military response. Vladimir Putin appears determined to destabilize the current world order and return Russia to its erstwhile superpower status, using a mix of soft and hard power. His active participation in the country's military exercises – including nuclear exercises – is regularly portrayed via video postings on YouTube in English, leaving little doubt that his intended audience goes well beyond Russian borders.

Russia has reverted to Cold War tactics such as incursions into NATO countries' air and sea space and the "buzzing" of NATO military aircraft and ships. The March 2014 annexation of Crimea and the November 2014 invasion of eastern Ukraine demonstrate Russia's intent to reassert its influence over former Soviet territories and test the NATO alliance. In 2016, the Ukrainian government accused Russia of orchestrating another highly sophisticated and coordinated cyber attack, this time on the country's electric grid, resulting in the loss of power throughout the country.

Like China, Russia's cyber units continue to penetrate U.S. government networks. They attempted to influence the U.S. presidential campaign of 2016 and exacerbate left-right divisions with a mix of social media trolling, false news reports, and the leaking of confidential emails. These tactics show no signs of abating.

In the energy sector, Russia's tactics include striking deals from China and Venezuela to Egypt, Iran, Turkey, and the Gulf countries. The objective is to reduce American influence and upset the balance of power. Europe's – especially Eastern Europe's – heavy dependence on Russian energy contributes to its unwillingness to respond to Russian aggression.

To reduce the dominance of U.S. and European energy companies, Russia is using social media campaigns to turn the public against nuclear power and fracking, while promoting green energy. Its financial backing of Green parties and environmentalist groups in both Europe and the U.S. is aimed at slowing down nuclear energy and natural gas production in the U.S. and halting any fracking development in Europe.

The risk of Russia expanding its sphere of influence to U.S. coalition partners in the Arabian Gulf holds particularly dire consequences. "The Russians are essentially buying their way into almost all the Middle Eastern Gulf Cooperation countries now. They're offering to put nuclear power plants in every one of them and pay the countries for the right to put them in. Who is going to cover the transfer of uranium outside these power plants to users who have other purposes in mind?"

Russia's Prime Minister, Vladimir Putin, uses a blend of soft and hard power in his campaign to return Russia to its erstwhile superpower status.

Photo courtesy of kremlin.ru

Kim Jong Un watches the test of a Pukguksong-2 intermediate-range ballistic missile.

Image courtesy of Korean Central News Agency

North Korea

North Korea has continued to defy sanctions and missile testing bans in recent years. The young, untested leader, Kim Jong Un, enjoys showing off his military with public parades of the armed forces and their weaponry. He uses state media to further his political aims and to threaten other countries with potential nuclear attacks. His actions risk setting off a regional arms race, and thus far, attempts to curb his ambitions with trade sanctions have not yielded much success.

Pyongyang's primary ally and trading partner, China, has enforced some of the sanctions, but has an interest in providing a softer response. North Korea shares a 1352-km-long border with China, which provides a buffer zone between China and thousands of U.S. troops stationed in South Korea. Moreover, should the current regime fail, China could face massive waves of hungry, displaced refugees. Russia, too, shares a border with North Korea, although it is much smaller. They could potentially play a bigger role in keeping North Korea in check, but so far, do not appear eager to do so.

Iran

Compared to the headline-grabbing antics of Kim Jong Un, Iran has been more discreet in its build-up of military power and influence. Despite protesting that its program is strictly for peaceful purposes, Iran's nuclear potential remains a threat to the U.S. and its allies, especially Israel. Iran continues to stir political discord throughout the greater Middle East region and engages in proxy wars by arming Shiite rebel groups – such as the Houthi in Yemen and Hezbollah in Lebanon – with advanced arms. The Houthi have regularly launched short- and long-range ballistic missile strikes at Saudi Arabia, the United Arab Emirates, and Abu Dhabi. The civil war in Yemen, pitting Saudi allies against Iranian allies, has become one of the world's worst humanitarian disasters, according to the United Nations.

Iran has had dozens of minor, but potentially dangerous, confrontations with the U.S. military in the Persian Gulf and the Strait of Hormuz, and they have increased over the past few years. While most incidents are simply harassment, there have also been attempts to threaten U.S. warships via close calls with Iranian vessels and threats by armed drones.

Islamic Extremism

While peer competitors and rogue regimes drive the national security agenda, there are still considerable and enduring threats from terrorist organizations. The U.S.-led coalition has steadfastly repelled Islamic State extremists from controlling vast regions in Iraq and Syria. The U.S. military and its allies have also been fighting to dislodge the Taliban and Al-Qaeda from significant portions of Afghanistan.

Despite suffering great losses in territory and casualties, Islamic terrorist groups have shown remarkable resilience and staying power. "If the United States Army had to absorb 70-, 80-, 90,000 killed in action in three and a half years, what would happen? This organization, this non-state actor that everybody hates – even our enemies hate ISIS – has absorbed that much physical damage, and they are still operating. It’s not over. That ought to make us think very hard about whether we understand the nature of this organization and its movement.” Islamic extremist groups, particularly Islamic State offshoots, continue to maintain strong footholds in Afghanistan and Pakistan, while gaining momentum in Indonesia, the Philippines, Sudan, Yemen, and parts of Africa.

The well-publicized brutal and vicious nature of the Islamic State continues to attract young men and women from around the world.

As disturbing as the barbaric methods of these terrorist groups are, it is their willingness and desire to inflict damage at an even greater scale that concerns the U.S. “One thing the Islamic State has proven is that if they can get their hands on something we would call WMD – like mustard, chlorine, sarin, or a nuclear device – based on what we've seen them do so far, they will absolutely use it.” Given the very nature of these terrorist organizations, an accumulation of tactical victories against them does not quickly translate into their strategic defeat.

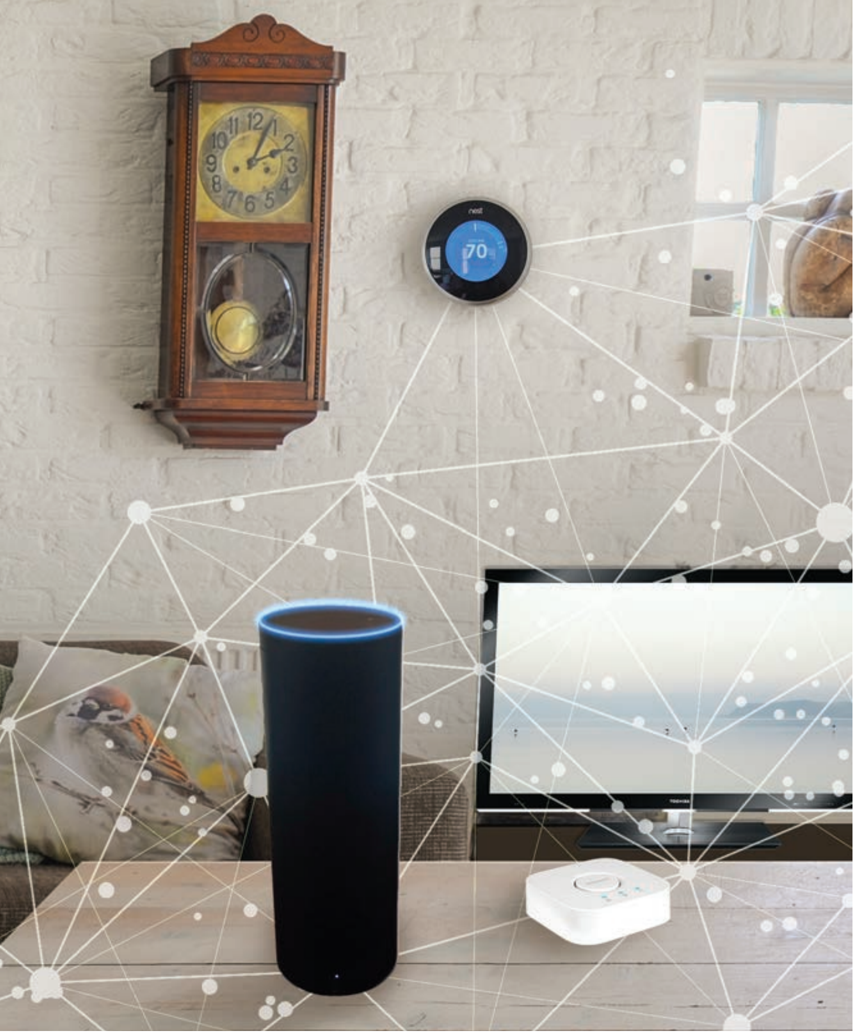
Demographic trends are such that prevention of ideological extremism is essential, though incredibly complex. “We've got to learn how to fight an idea that's associated with a huge youth bulge around the world, and is driven by enormous unhappiness and dissatisfaction among those who are tempted to take the radical path.”

Can the U.S. Protect Its Open Society?

While acts of terrorism in Europe and the U.S. receive ample publicity, most Americans remain largely unaware of the volume and variety of threats the U.S. faces today. The military is currently engaged in 150 countries, mostly unnoticed by the public and underreported by the press. The U.S. has suffered a relatively low number of casualties, so these conflicts do not garner much media attention. This contrasts with the large engagements of the 20th century, when the greater part of the American public was personally involved. The draft lasted throughout the two World Wars, the Korean War, and the Vietnam Conflict, so almost all had friends or relatives who served. Today, the all-volunteer military is a professional, better-trained force, but the end of the draft has meant that far fewer Americans are familiar with military operations, and therefore few understand the urgent need to invest in modernization.

The national security community has been doing a good job of identifying and mitigating threats

Can the convenience and freedom of modern U.S. society persist in the current threat environment?



With the advent of the Internet of Things (IoT), which connects personal information to everyday devices, a whole new category of vulnerability is opened.

early on, before they become tragedies. Since most of the preventive work the Intelligence Community and the Department of Defense perform remains classified, the public is unaware of the number and kinds of threats that were averted. This includes elected officials, who often remain unconvinced of the need for increased national resources, both human and financial. “Our leaders don’t say that we have threats of this magnitude. They don’t say that our military is not capable of doing things that the American public takes for granted it can do. And therefore, people don’t know.”

The 2011 Budget Control Act made modernization of platforms and troop readiness very difficult to achieve. The most recent budget bill remedied some of the shortfall. However, today’s parties are much wider apart in their views of problems and priorities compared to decades past, and compromise is seen by their core voters as “selling out.” These political divisions are not lost on adversaries, who are quick to take advantage of them.

As noted, Russia has been especially adept at fomenting and exacerbating political disunity. Americans were caught off guard when several “news” and social media websites were revealed to be run by Russian agents. The discovery that information operations by adversaries could sway public opinion and potentially affect election outcomes eventually led the largest social media platforms to try to flag and remove foreign propaganda, as well as hate groups. However, calls continue for greater monitoring of online content, due to its ability to reach a wide audience.

Easy online access to personal information about American citizens makes them attractive targets for identity thieves, whether military adversaries or mere criminals. Unlike Europe, where stricter online privacy laws are in place, information about American residences, family members, and more is found online with a simple search. As sharing information and even locations on social media sites becomes more popular, profiling targets is made even easier.

With the advent of the Internet of Things (IoT), which connects personal information to everyday devices, a whole new category of vulnerability is opened. As IoT technology spreads into businesses, utilities, government agencies, and even military platforms, these vulnerabilities pose a risk to national security. IoT operating protocols were designed for convenience and ease of networking, not security. Generally too small to enable encryption or allow security updates, they are easy prey for cyber thieves and foreign governments alike.

U.S. utilities, especially the smaller rural cooperatives, have an urgent need to address IoT, network, data, and physical plant vulnerabilities. Unlike in China and Russia – and most of Europe – most U.S. companies are in private hands. Both the electricity grid and water supply depend on the capability of these large and small utilities to defend themselves against attack. With so many different companies and oversight boards, assessing their state of readiness and resilience is a complicated task.

The Internet itself is akin to a utility where continuous service is relied on and expected by business, government, and consumers. Yet in contrast to China, North Korea, Iran, and Russia, the U.S. government has no control of the Internet Service Providers, the flow of information over the Internet, or the networks.

The Threat of Low-Cost Technology

Inexpensive, commercially available technology has changed the threat landscape and the U.S. ability to defend itself and its allies. With reference to the Observe, Orient, Decide, Act (OODA) operational loop of warfare, "We used to own the OO part of the loop: we had the night vision and sensors, but now the field is leveling with commercial items, including satellite surveillance. These satellites can't [yet] read license plates, but they can identify cars and models."

Adversaries can now perform surveillance and inflict damage at a relatively low cost. Barriers to access have been lowered, and modern technology has become so easy to use that even unsophisticated groups with little access to cash can pack a punch. For example, the burgeoning popularity of drones has led to advances that have caused the price of unmanned aerial vehicles (UAVs) to drop below $1,000. "If you think about how ISIS used drones initially, they started out as a reconnaissance platform. They then moved to become a reconnaissance platform that was essentially capable of vectoring a pinpoint device, such as a vehicle-borne IED. Now they have been made into a device that can drop a 40-mm grenade on a known position."

For years, the U.S. "owned the night" with advanced night vision equipment. Commercially available technology has greatly diminished that asymmetric advantage.

2 Evolving Roles and Missions in the Global Threat Environment: What Will It Take to Prevail?

The U.S. has reached a critical juncture. The proliferation of threats the nation faces has made the national security mission more complex than ever. China and Russia have modernized their systems and capabilities, surpassing the U.S. in several areas. North Korea and Iran pose threats to regional stability, and radical Islamic terrorist groups continue to inflict physical and psychological damage around the world. Cyber attacks, the probing of national infrastructure and defenses, the wholesale theft of technology, and military aggressions throughout the world continue unabated. Despite the number of attacks by adversaries and their growing capabilities, the American public seems to have little sense of urgency or awareness that hostilities are already underway. “Our paradigm for what it means to be at war is outdated, and we are missing the fact that others are at war with us. Our expectation in the international order is that the norm is peace.”

The U.S. must continue to adapt to the new global competitive environment and anticipate what lies ahead. Failures of the past have frequently been failures of imagination – often caused by overconfidence and the desire to rest on the laurels of past successes, as well as overreliance on comfortable assumptions. The U.S. did not anticipate the new asymmetric threat environment, did not imagine what the future might hold if no action was taken, and did not foresee the reactions brought about by necessary actions that were taken.

America needs thinkers who have the courage to stand up and propose bold solutions in technology, diplomacy, and operations. This will require leaders without preconceived notions, who are willing to address the world as it is, not how we wish it to be – leaders capable of thinking broadly and encouraging healthy debate. “We need leaders that can think through problems, that can take information, discern what’s chaff and what’s wheat, and make a cogent decision. We need to create people who can think, who can ask tough questions. The greatest asymmetric advantage is our ability to think through problems, because nobody in this room knows what the future looks like. No matter what we plan, it’s going to be different.”

The type of wars the U.S. will face cannot always be foreseen, so preparation must include every possible scenario, across domains. It is irresponsible in the extreme to expect adversaries to cooperate and play to America’s strengths. “If we’re going to maintain our position as the world’s sole superpower, we need to be able to fight and succeed across the spectrum of conflict.”

> “Nobody in this room knows what the future looks like. No matter what we plan, it’s going to be different.”

Deterrence Through Dominance Across All Domains

With so many asymmetric threats facing the country, the U.S. must deter aggression by the credible potential of an overwhelming response and, if deterrence fails, fight to win wherever and whenever necessary. “Remember: deterrence is not what you or I think; it’s what the adversary thinks. And deterrence is made up of two things: the capability and the will to use it. We can develop the capability, but we have to have the will to use it, the will that the Russians believe, the Chinese believe, and the North Koreans believe.” Critical to deterrence is the perceived will to act, as well as the strength of America’s forces, both nuclear and conventional, including the space and cyber domains.

Until a few years ago, space was considered a peaceful sanctuary of international scientific cooperation, and space battles were the stuff of science fiction. As adversaries make strides in the militarization of their space capabilities, space has become yet another contested domain: “Space capability is absolutely foundational. The President of the United States needs to be able to communicate with all fielded forces 24 hours a day, seven days a week, and we need to know if somebody is launching something at us."

Also critical is the functioning of Global Positioning Systems (GPS), or Precision Navigation and Timing (PNT) systems, which enabled the development of precision munitions and revolutionized military operations. Their adoption spread quickly through the civilian world, radically changing business. Today's PNT satellite systems are no longer primarily a mapping convenience: everything from gas stations to banks relies on these systems. Protecting these and other systems from nefarious actors in space and cyberspace has become critical to U.S. economic well-being, as well as to its ability to conduct military surveillance, reconnaissance, and operations.

Cyber and electronic warfare capabilities are also essential for deterring and defeating adversaries. This includes protecting networks and infrastructure, launching attacks from inside adversary networks and platforms, and simply taking down the enemy's ability to communicate and fire weapons during battle. There is no question that cyber and electronic warfare capabilities are changing the character of war itself, and America cannot afford to fall behind.

The most powerful deterrent against an attack on the nation's soil remains America's nuclear strength. The doctrine of "mutually assured destruction" has functioned as an insurance policy against all-out war for almost 70 years. However, as more and more countries acquire nuclear capability, the risk of nuclear employment grows proportionately. For the nuclear triad to remain an effective deterrent, the U.S. must continue to invest in the technology and train the next generation of scientists. "To say we need to modernize our systems is an understatement. Our nuclear forces were developed in the 1960s. Our modernization programs are late. If anything keeps me up at night, it's making sure we have the intellectual capital to think about this in the future, because we took a holiday. Russia and China did not take a holiday."

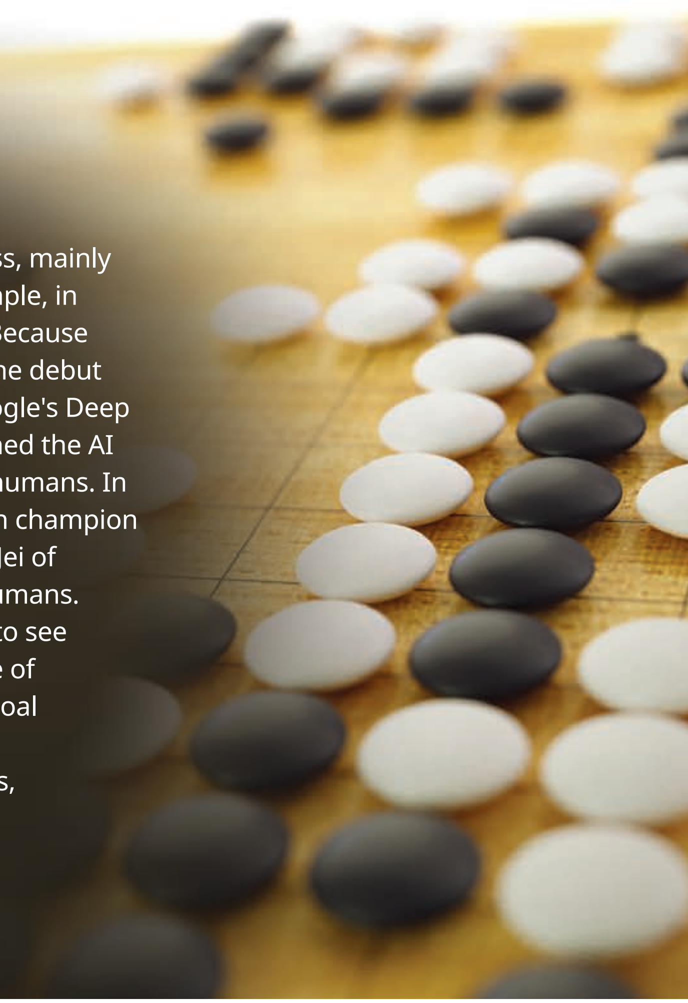
North Korea and Iran have not taken a timeout, either. "North Korea is acquiring nuclear weapons so that every discussion we have with them in the Pacific region will be about a nuclear conflict, whether anybody shoots or not. That's why the stakes are so high." The U.S. considers nuclear conflict a last resort that risks an all-out escalation. The extent to which this notion is shared by other regimes – particularly the "Hermit Kingdom" that is North Korea – is much less clear. Even Russia – with whom the U.S. has signed numerous arms control and reduction accords – is believed to have evolved a new doctrine of "escalate to deescalate" – meaning they could employ a (relatively) low-yield nuclear weapon early in the conflict, based on the assumption that the U.S. would shy away from massive retaliation.

> "To say we need to modernize our systems is an understatement. Our nuclear forces were developed in the 1960s."

Modernization Is Essential Across All Domains

Updating the U.S. nuclear triad is an extraordinarily expensive yet vital undertaking. The only higher cost than preventing a nuclear conflagration is engaging in one. Escalation control – and the ability to threaten such great damage on any adversary that any possible gain is thoroughly negated – is the essence of deterrence. Nuclear weapons have remained a taboo since their single employment to end World War II in August, 1945. It behooves the world to retain that taboo.

Conventional weaponry also requires modernization. Continuous deployments have taken a toll on platforms in every service, which now require much more frequent maintenance. The process for developing and delivering new platforms and capabilities is slow and cumbersome, fraught with delays and budgetary constraints. In the meantime, China and Russia are building more platforms with advanced



AI Platform Makes History

The ancient Chinese game of “Go” is much more complex than chess, mainly due to the sheer number of possible moves on the board. For example, in chess, there are 20 possible opening moves, whereas Go has 361. Because it has so many potential moves and its strategies are so nuanced, the debut of a computerized Go player seemed to be a distant goal. Then Google's Deep Mind artificial intelligence (AI) group developed AlphaGo. They trained the AI platform using a huge database of thousands of games played by humans. In 2016, AlphaGo shocked the Go community by beating South Korean champion Lee Sedol 4-1. Then in 2017, AlphaGo defeated world champion Ke Jei of China. After the victory, AlphaGo retired from playing Go against humans. Deep Mind then created a new version they dubbed AlphaGo Zero to see if the program could learn how to win all by itself. With no database of games to learn from, its only input was the rules of the game, the goal of winning, and feedback on its success. Starting from completely random play, it played millions of games against itself. In three days, it reached master level, and in 40 days, AlphaGo Zero defeated the original AlphaGo, essentially becoming world champion. Most exciting, the program showed that machines, like humans, can learn “tabula rasa,” without the need for human data sets.

capabilities, and North Korea continues to test its missile systems and the U.S. response.

Delivery of any weapon across the globe requires the ability to communicate, so the importance of dominating the electro-magnetic spectrum cannot be over-stated. Radar, PNT systems, computers, and communications all depend on the electro-magnetic spectrum. “Electronic warfare is key. We need to own the spectrum.”

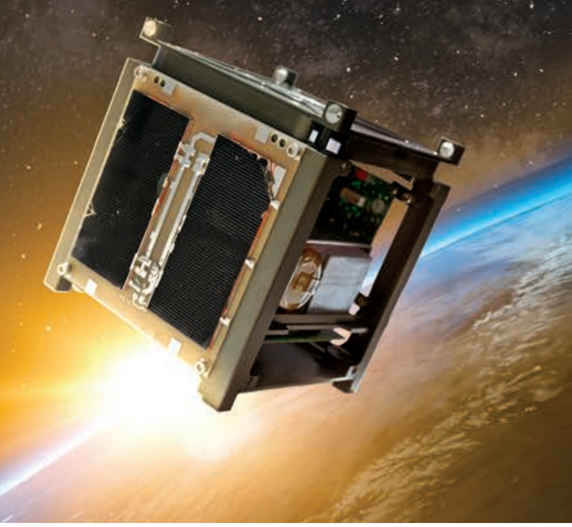
Essential to any platform or system is resilience: adversaries will do all they can to damage American systems. The U.S. must be able to fight through a coordinated attack. “We have to get better at thinking about the resilience of the architecture that we’ve put together. It requires us to think creatively on whether we think it can weather a bad day. Sometimes resilience can be the product of diversity of capabilities.”

Desired effects will increasingly be attained through the interaction of multiple capabilities, each sharing information for a common purpose. “No longer is it sufficient to focus on managing just the physical elements of a conflict – the planes, satellites, troops, ships … These systems are evolving to a much more highly integrated enterprise collaboratively leveraged through the broad exchange of information.” The sharing of information as part of a strategy to expand capabilities includes allies and coalition members. “The seamless sharing of information will enhance our combined effectiveness, while compensating for the vulnerabilities of each, and we need to do that inside an adversary’s decision loop.” The U.S. cannot afford to act alone, but allies and coalition partners often cannot afford U.S. technology. “We’ve got to broaden the Five Eyes Partnership [which includes the U.S., U.K., Canada, Australia, New Zealand]. We’ve got to bring the capacity and capability of other nations to help us fight the adversary.”

Dominance of surveillance and targeting technology once gave the U.S. an asymmetric edge on the battlefield, but commercial technology has almost flattened it. “We used to own the all-weather, all-circumstances night

Satellites the Size of a Rubik’s Cube

Military operations depend on reliable communications, so the development of small-form-factor satellites has garnered great interest. These so-called nanosatellites can be as small as a Rubik’s cube and are usually launched as a secondary payload during regular satellite or space mission launches. Initially used primarily for academic research, the relatively low cost of building and launching these and other nanosatellites has made them highly attractive to military planners. Nanosatellites can be used to collect and transmit weather data, communications, and imagery. For troops in remote locations with no over-the-horizon communications, having a resilient network of low-cost, low-orbit satellites could be key to survival.



vision. No more.” The erosion of this decisive advantage puts greater emphasis on increasing the speed at which operators decide how to respond. “The actions required to defeat or respond to a threat are so much quicker today than they’ve ever been.” In cyber warfare, where millisecond responses are called for, automated responses are needed at low thresholds. In all domains, machine learning and artificial intelligence can assist with the identification of threats, suggest responses, and calculate likely responses. In the American mindset, however, any decision that causes great harm or death must ultimately come from humans. As artificial intelligence and man-machine teaming proliferate, it must be considered whether – and with what effect – less scrupulous adversaries might cede lethal decisions to machines.

Decision windows must shrink even further, with decisions increasingly pushed down and out to lower, less centralized echelons. “A pretty powerful concept being thrown around is this idea of commander’s intent and feedback. How do you communicate that intent, let your teams go out and do what they need to do, and then count on them to inform you of what matters?”

The principle of enabling those closest to the problem to decide the best course of action has merit beyond the battlefield. With military and government competing with industry – including Silicon Valley – for the “best of the best” in personnel, it is essential to allow troops and employees the opportunity to try novel approaches to problems. The tendency of the mid-tier of government bureaucracy is to avoid risk and, therefore, to say “no” to anything new. This risk-averse and stale mentality demotivates the best employees and troops and negatively affects retention rates.

With the number of U.S. troops today at roughly half that of the 1990 Armed Forces, and the fast operations tempo experienced since then, incentivizing experienced personnel to remain in the service is indispensable. One-size-fits-all measures will not suffice: “We need to allow our personnel to prioritize what matters most to them, in terms of location, education, and compensation.” Compensation cannot be reduced to mere monetary terms. Leaders must ensure that troops are receiving enough rest, training, and family time, along with opportunities to tackle challenges in new ways and allow room for failure on the path to success: “We need to allow people to test, fail, and test again. That’s how you develop innovation, because people won’t be afraid to try something and fail.”

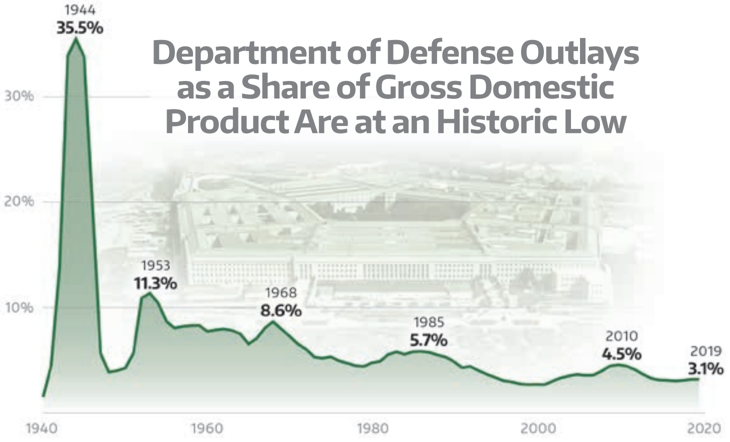
Urgent Need to Rethink Acquisitions and Delivery

Excessive bureaucracy and risk aversion are the antithesis of innovation. While adversaries have picked up the pace of achieving advanced capabilities, the U.S. often remains mired in a lengthy procurement cycle. If the U.S. plans to maintain an edge in the realm of fast-changing technology, there must be a willingness to accept calculated risks: “We need a way to take chances, fail fast, and off-ramp those things that fail fast, then take what we’ve learned from these failures, as we did in the 50s and 60s, and roll them into the next development.”

The current drawn-out system of requirements identification, development, testing, and manufacturing cycles must change. It is urgent that the U.S. government streamline its acquisitions processes and reward its personnel and industry partners for innovation. “At one point in time, government developed technological capabilities that exceeded those of commercial space. That equation is now reversed.” New technologies such as artificial intelligence, hypersonic vehicles, quantum computing, and directed energy hold great promise for ensuring our military edge, but tapping into their benefits requires accelerating delivery and deployment. “We need to speed development in the R&D process. We can’t stay with the traditional methodologies we’ve been using.”

Simplifying and shortening the process is the right path economically, as well, because the current complexity of the procurement system balloons costs for the government and negatively affects the bottom line for industry. Greater agility is fundamental. One solution put forth is to narrow the scope of certain acquisitions: “It may not be ‘sell me a solution,’ or ‘sell me a device.’ Maybe it’s as simple as the math. Maybe it’s the science. Maybe it’s just the algorithm that drives the process, and how do you put that on an existing system to defeat that emerging threat?”

Adversaries and nation-state competitors are closing the gap with the U.S. in terms of military technology, but the strength of the U.S. economy remains an asymmetric advantage. “The gross domestic product (GDP) of a country represents its power. It finances its military. It adds to the quality of life. It provides education. We are in the catbird seat: I would not take anybody’s cards over ours.” In terms of GDP, the U.S. continues to shine, standing at about $18.5 trillion. China, with roughly three times the population, has a GDP of $11 trillion, while Russia lags at $1.3 trillion and North Korea, a mere $28 billion. “North Korea is seeking an asymmetric edge to try to level the playing field through the development of nuclear weapons, and we need to understand that.”


Department of Defense Outlays as a Share of Gross Domestic Product Are at an Historic Low

When it comes to non-state terrorist groups, the U.S. and coalition partners have been successful at driving them out of their territories and have made great strides in following the trail of finance that supports their activities. Still, as one group is defeated, another arises. No solution will be sufficient unless some of the historic, social, and economic root causes are fully understood, and there is a concerted effort to focus on prevention. Lack of economic opportunity is a key driver, as is allegiance to ethnic, religious, and tribal entities, rather than to the official government. “It should not surprise us that when a non-state actor can offer a more effective alternative than the government, people shift allegiance.”

Fighting an ideology that has taken the form of a generational religious battle does not belong strictly in the military realm. Every death suffered, every home destroyed regenerates hatred and renews violence. Diplomacy, education, and above all, communication of a better ideal by which to live are essential – and a great challenge to America today.

3 Conclusions

Protecting U.S. interests has never been an easy task. China, Russia, North Korea, Iran, and terrorist organizations have all been watching the U.S. very closely for years. Deterring these adversaries and overcoming the full range of threats facing America requires a holistic approach. To prevail, the U.S. needs to stand united as a nation and forge close ties with allies and coalition partners. Leaders must be honest with the public that the risks are many, the situation is complex, and there are no simple answers. It is crucial to harness the talent of industry, government, the military, and academia to work together to find novel ways to develop technology, make faster decisions, and reward risks on the path to success. "It's everybody's job to protect the country."

Time is of the essence. It is critical that leaders work together across institutions to address these threats. Unaware of all that is at stake, many are skeptical about the need for a more robust defense to deter aggression and are unwilling to bear the high costs of the long-overdue modernization needed for conventional and nuclear platforms.

> "It's everybody's job to protect the country."

Political differences must not diminish the ability to budget and plan for current and future defense: "We have to come to some type of agreement, so we all understand what kind of war we might have to fight." The roles of diplomacy and intelligence should not be ignored, because only a deep understanding of the threats and a unified approach to overcoming them will allow the U.S. and its allies to maintain the edge and deter those who seek to upend the world order for their own gain.

To prevail against the rapid advances of nation-state adversaries and terrorist groups, the U.S. must stand united as a nation and forge close ties with allies and coalition partners.

Photo courtesy of Kevin Rutherford

ACKNOWLEDGEMENTS

Symposium Participants (in alphabetical order)

Rear Admiral Paul B. Becker, USN (Ret)
Senior Fellow, Center for Naval Analysis,
University of Virginia's Batten School
for Leadership and Public Policy

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

Lt Gen (Ret) Deptula also served as Advisor

Major General John G. Ferrari, USA
Director, Program Analysis and Evaluation
Office of the Deputy Chief of Staff, U.S. Army

Frank J. Gaffney
President, Center for Security Policy

Mr. Gaffney also served as Advisor

The Honorable James S. Gilmore III
Former Governor of the
Commonwealth of Virginia

Major General Steven R. Grove, USA
Vice Director, Joint Improvised-
Threat Defeat Organization

Lieutenant General Anthony R. Ierardi, USA
Director, Force Structure, Resources
and Assessment, Joint Staff

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

Dr. Kagan also served as Advisor

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

Dr. Kass also served as Advisor

Vice Admiral Andrew L. Lewis, USN
Deputy Chief of Naval Operations
Information, Plans and Strategy, U.S. Navy

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

Major General James R. Marrs, USAF
Assistant Deputy Chief of Staff
for Intelligence, Surveillance, and
Reconnaissance, U.S. Air Force

Brigadier General Joseph P. McGee, USA
Deputy Commander for Operations,
U.S. Army Cyber Command

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

Lieutenant General Mark C. Nowland, USAF
Deputy Chief of Staff, Operations, Plans
and Requirements, U.S. Air Force

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

Dr. Phillips also served as Advisor

Admiral John M. Richardson, USN
Chief of Naval Operations, U.S. Navy

Lieutenant General
Anthony J. Rock, USAF
Inspector General of the U.S. Air Force

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

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

General Stephen W. Wilson, USAF
Vice Chief of Staff of the U.S. Air Force

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

Advisors

Ken Asbury
President and Chief Executive Officer,
CACI International Inc

Jody Brown
Executive Vice President,
Corporate Communications,
CACI International Inc

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

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

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

Symposium Support Team

Event Manager

Erica Davis
Marketing Administrator,
CACI International Inc

Participant Coordinator

Casey Pierce
Business Analyst,
CACI International Inc

Report Lead

Tricia Branagan
Strategic Communications Lead,
CACI International Inc

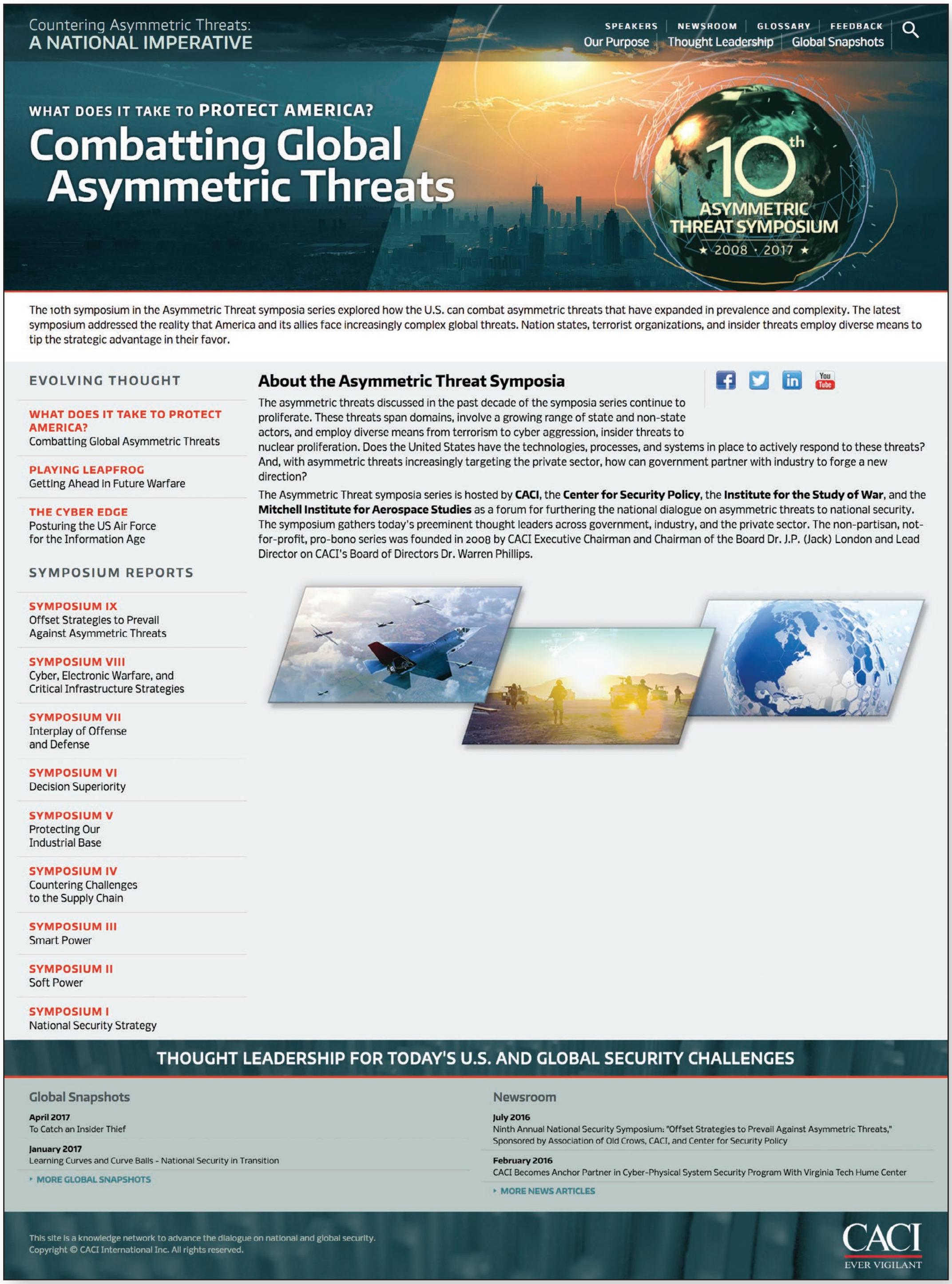
Editors

Erika Glon
Director, Marketing,
CACI International Inc

Michael Pino
Publications Principal,
CACI International Inc

Art Direction and Graphic Design

Chris Impink
Lead Multimedia Designer,
CACI International Inc


Countering Asymmetric Threats:
A NATIONAL IMPERATIVE
SPEAKERS | NEWSROOM | GLOSSARY | FEEDBACK
Our Purpose | Thought Leadership | Global Snapshots
10th
ASYMMETRIC THREAT SYMPOSIUM
★ 2008 · 2017 ★

WHAT DOES IT TAKE TO PROTECT AMERICA?

Combatting Global Asymmetric Threats

The 10th symposium in the Asymmetric Threat symposia series explored how the U.S. can combat asymmetric threats that have expanded in prevalence and complexity. The latest symposium addressed the reality that America and its allies face increasingly complex global threats. Nation states, terrorist organizations, and insider threats employ diverse means to tip the strategic advantage in their favor.

EVOLVING THOUGHT

WHAT DOES IT TAKE TO PROTECT AMERICA?
Combatting Global Asymmetric Threats

PLAYING LEAPFROG
Getting Ahead In Future Warfare

THE CYBER EDGE
Posturing the US Air Force
for the Information Age

SYMPOSIUM REPORTS

SYMPOSIUM IX
Offset Strategies to Prevail
Against Asymmetric Threats

SYMPOSIUM VIII
Cyber, Electronic Warfare, and
Critical Infrastructure Strategies

SYMPOSIUM VII
Interplay of Offense
and Defense

SYMPOSIUM VI
Decision Superiority

SYMPOSIUM V
Protecting Our
Industrial Base

SYMPOSIUM IV
Countering Challenges
to the Supply Chain

SYMPOSIUM III
Smart Power

SYMPOSIUM II
Soft Power

SYMPOSIUM I
National Security Strategy

About the Asymmetric Threat Symposia

The asymmetric threats discussed in the past decade of the symposia series continue to proliferate. These threats span domains, involve a growing range of state and non-state actors, and employ diverse means from terrorism to cyber aggression, insider threats 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 Asymmetric Threat symposia series is hosted by **CACI**, the **Center for Security Policy**, the **Institute for the Study of War**, and the **Mitchell Institute for Aerospace Studies** as a forum for furthering the national dialogue on asymmetric threats to national security. The symposium gathers today's preeminent thought leaders across government, industry, and the private sector. The non-partisan, not-for-profit, pro-bono series was founded in 2008 by CACI Executive Chairman and Chairman of the Board Dr. J.P. (Jack) London and Lead Director on CACI's Board of Directors Dr. Warren Phillips.

THOUGHT LEADERSHIP FOR TODAY'S U.S. AND GLOBAL SECURITY CHALLENGES

Global Snapshots

April 2017
To Catch an Insider Thief

January 2017
Learning Curves and Curve Balls - National Security in Transition

‣ MORE GLOBAL SNAPSHOTS

Newsroom

July 2016
Ninth Annual National Security Symposium: "Offset Strategies to Prevail Against Asymmetric Threats," Sponsored by Association of Old Crows, CACI, and Center for Security Policy

February 2016
CACI Becomes Anchor Partner in Cyber-Physical System Security Program With Virginia Tech Hume Center

‣ MORE NEWS ARTICLES

This site is a knowledge network to advance the dialogue on national and global security.
Copyright © CACI International Inc. All rights reserved.

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.