

Countering Asymmetric Threats:  
A National Imperative

# Decision Superiority: Countering Surprise, Denial, and Deception

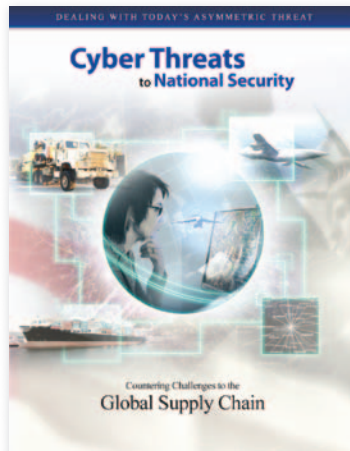


The Asymmetric Threat website ([asymmetricthreat.net](http://asymmetricthreat.net)) includes downloadable reports from all symposia in both series and serves as a knowledge network to advance the dialogue on national and global security, presenting resources and original research, and providing a forum for review and discussion of pertinent themes and events.

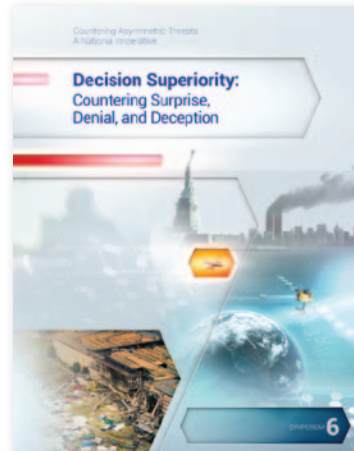
#### SERIES ONE



#### SERIES TWO



#### SERIES THREE



This document is intended only as a summary of the personal remarks made by participants at the May 8, 2012 symposium, *“Decision Superiority: Countering Surprise, Denial, and Deception,”* held at the U.S. Navy Memorial, Washington, D.C., and co-sponsored by CACI International Inc (CACI), the U.S. Naval Institute (USNI), and the Center for Security Policy (CSP). Invocation of the Chatham House Rule established the symposium and report as non-attribution forums.

This report is published as a public service. It does not necessarily reflect the views of CACI, USNI, CSP, the U.S. government, or their officers and employees.

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. CACI and the National Defense University sponsored Symposium One in the series, and CACI and USNI sponsored Symposia Two and Three. Symposium Four initiated a new Asymmetric Threat series focusing on Cyber Threats. CACI and USNI sponsored Symposium Four and CSP joined as a sponsor for Symposium Five. Symposium Six now initiates a new series focused on the requirements and means for the U.S. to achieve decision superiority.

*September 2012*



# Table of Contents

Executive Summary .....	3
1 › Lessons of Surprise, Denial, and Deception .....	5
2 › Are Surprise and Deception Preventable? .....	7
3 › Leadership, Authorities, and Decision-Making .....	10
4 › Strategic Implications .....	13
5 › National Imperatives Moving Forward .....	16
6 › Conclusion .....	20



Battle of Jericho, ca. 1400 BC

Battle of Trenton, 1776

Invasion of Poland, 1939

# Executive Summary

On May 8, 2012, CACI International, the U.S. Naval Institute, and the Center for Security Policy held *Decision Superiority: Countering Surprise, Denial, and Deception*, a symposium dedicated to national discourse on prominent national security challenges. This report reflects the presentations and discussions held by prominent keynote speakers, panelists, and audience members.

Surprise, denial, and deception are as old as war itself. Throughout history, adversaries have been outmaneuvered on battlefields. Policy makers have failed to anticipate socio-economic and political crises worldwide. Both man-made and natural disasters continue to expose unpreparedness for such events. Cyber technologies, used either in stand-alone attacks or as force multipliers, add a new dimension to the challenge. It can be argued that surprise, denial, and deception are the ultimate asymmetric threats because they expose vulnerabilities and interfere with assessment and decision-making

while influencing – even shaping – policies and the balance of power. Often dismissed as “weapons of the weak,” surprise, denial, and deception also exploit systemic vulnerabilities, vanity, and self-delusion. While surprise, denial, and deception are traumatic and humiliating to the target, they only create a temporary advantage to the initiator. It is, however, up to the target to recover and respond, or become a victim.

Because surprise, denial, and deception are psychological phenomena, they cannot be prevented. Surprise, denial, and deception are successful because they challenge the perceptions that fill the very large gap between what is known and unknown. Observations and events are filtered through a prism of culture, assumptions, biases, and experiences, leading actors to mistake the unfamiliar with the improbable. This explains why collecting vast amounts of data does not necessarily lead to better situational awareness and decision superiority.

Warning is a vital link connecting intelligence assessment with countermeasures and other preparations. However, warning systems are also subject to biases, preconceptions, and other human factors that encumber decision-makers. An accurate understanding of the capabilities and limitations of C4ISR<sup>1</sup> is, therefore, essential in countering surprise, denial, and deception.

The institutions, authorities, and processes designed to deal with surprise, denial, and deception are not necessarily equipped to handle them, due to factors ranging from information overload to interagency bureaucracy. Changing the national security infrastructure in the U.S. to adapt to these challenges would be a monumental task, but innovative and cooperative efforts across responsible organizations are already underway.

The strategic implications of mitigating surprise, denial, and deception are considerable. The inability to transform organizations, adopt new operational concepts, or leverage breakthrough technologies reveals systemic failures to anticipate, learn, and adapt. Threats range from the immediate to the crippling and existential. The future national security environment will be shaped by the interaction of globalization, economic disparities,



**Surprise, denial,  
and deception are  
as old as war itself.**

*Images courtesy of the German  
Federal Archive; the Federal  
Emergency Management  
Agency; and public domain*

<sup>1</sup> Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

and competition for resources; diffusion of technology and information networks and devices whose very nature allows unprecedented ability to target, harm, and potentially paralyze advanced nations; and systemic upheavals impacting state and non-state actors and, thereby, international institutions and the world order. The U.S. and other nations are bound to confront these challenges wherever they engage to promote and defend their interests.

Moving forward, national security leaders will be faced with both challenges and opportunities in countering surprise, denial, and deception. First, it will be necessary to cultivate better ways of thinking, from observation to assessment.

Existing perspectives and paradigms that still rest heavily on symmetric and preventive thinking will have to embrace empathy and improve the understanding of adversaries' cultures, perspectives, and interests. This will also mean creating an environment where such different insights and ideas are seriously considered and incorporated throughout U.S. national security organizations.

Second, leaders should prioritize and promote investments in people and technologies, capitalizing on knowledge and capabilities that are readily adaptable to handling new threats. There is also discussion about moving away from network-centric to knowledge-centric systems to better counter asymmetric threats.

Third, national security leaders will need to leverage partnerships across government, with other nations, and with the private sector. Since 9/11, various agencies have come together to protect the country. However, interagency cooperation will still have to overcome many organizational and cultural obstacles to fully capitalize on existing knowledge, skills, and relationships. Global challenges will require global responses. International partnerships will not only have to be more innovative, but also include regions where close relationships have not traditionally existed before. Finally, the private sector should also be seen as a key partner with the government in absorbing, rebuilding, and reconstituting capabilities from such multi-faceted asymmetric attacks.



**The future national security environment will be shaped, in part, by the diffusion of technology and information networks and devices whose very nature allows unprecedented ability to target, harm, and potentially paralyze advanced nations.**

*Graphic courtesy of CACI*



# 1 Lessons of Surprise, Denial, and Deception

Surprise, denial, and deception are some of the oldest tricks in the book. As the combination of information superiority and decisive action, decision superiority will be achieved by better understanding of threats, improving resilience, and fuller integration of the perspectives and players in national security. Otherwise, nations risk falling for the same old tricks.

Surprise, denial, and deception can justifiably be described as “the ultimate asymmetric threats.” They interfere with the ability to assess adversaries’ intentions and capabilities, and respond to threats. They impede the ability to make timely and optimal decisions, as well as account for one’s own vulnerabilities. They influence policies and public opinion and can shift the balance of power by shaping perceptions in an adversary’s favor. Unable to take their opponents head on, asymmetric actors rely on the force-multiplying effects that the shock and psychological dislocation of surprise inevitably produce. Furthermore, deliberate attempts to surprise and deceive rarely fail.

Defeating the threats from surprise, denial, and deception, and checking this critical asymmetric advantage require a thorough understanding of their nature, as well as the resolve to develop the means necessary to minimize their impact and consequences.

---

**“History has not been a good teacher. Superpowers, small nations, and non-state actors have all deliberately deceived and been deceived, surprised others, and fallen victim to surprise.”**

---

Surprise, denial, and deception are as old as war itself. Biblical warriors and kings practiced surprise attacks, ruses, and guiles. A millennium later and a continent apart, their virtues were recognized and extolled as “the strategist’s key to victory” in Sun Tzu’s *Art of War*. From ancient Persia, Greece, and Rome, through two World Wars, and now into the early 21<sup>st</sup> century, nations and non-state actors have practiced surprise and deception, and have fallen victim to them – often with devastating consequences.

Each of the great powers involved in World War II was both a victim and a perpetrator: the British were surprised

by the German invasion of Norway; the French by the German invasion of their country; the Americans by Pearl Harbor; and the Germans by the Allied landings in Normandy. The best intelligence services and most elaborate warning systems have failed to predict war. The Soviet leadership was surprised by the German invasion of June 1941. Israeli intelligence, considered one of the very best, failed to anticipate the Arab attack of October 1973. The record since has not improved much, including the December 1979 Soviet invasion of Afghanistan, the September 1980 Iraqi attack on Iran, and the August 1990 Iraqi attack on Kuwait. Until September 11, 2001, few Americans were aware that Al Qaeda had publicly declared war on the U.S. Likewise, Operations Desert Storm, Allied Force, Enduring Freedom, Iraqi Freedom, and Odyssey Dawn (Libya) – to note some of the better-known recent campaigns – all involved successful surprise and deception activities.

**Troops of Company E, 16<sup>th</sup> Infantry, 1<sup>st</sup> Infantry Division (the Big Red One) wading onto Omaha Beach during the Normandy landings on the morning of June 6, 1944.**

*Photo courtesy of U.S. Coast Guard*





**Decoys used in the Operation Fortitude deceptions and buildups for D-Day included realistic-looking weapons like this inflatable tank.**

*Photo courtesy of U.S. Army*

Policy-makers have also failed to anticipate and prepare for global crises. This includes such key events as the fall of the Shah in Iran and the ensuing hostage crisis, the collapse of the Soviet Union and the Warsaw Pact, the genocides in Rwanda and Sudan, the rise of violent Islamist extremism, and the recent events of the “Arab Spring,” as well as the current worldwide economic downturn.

Man-made and natural disasters have revealed flaws and gaps in

disaster preparedness, cross-sector coordination, and relief operations. Examples include nuclear reactor meltdowns at Chernobyl (Ukraine, 1986) and Fukushima (Japan, 2011), oil spills (Exxon in 1989 and BP in 2006), and Hurricane Katrina (U.S. Gulf Coast, 2005).

Cyber operations span the range of surprise, denial, and deception. Some are clearly deliberate military attacks (e.g. Russia’s on Georgia prior to its 2008 invasion); some accord

plausible deniability and strike at the intersection of force and diplomacy (e.g., the Stuxnet attacks on Iran’s nuclear production facilities, which, perhaps for the first time in history, physically destroyed infrastructure without using kinetic force); and others remain unattributed or undisclosed.

As one Symposium Six participant stated, “The world is awash with surprises, some of which are very strategic in character, some of which could be, some of which simply change the nature of the tactical situation we confront.” Whether small or large in degree, as a force-multiplier or on their own, surprise, denial, and deception are game-changers for which the U.S. and other nations must be better prepared.



**Man-made disasters, such as the Chernobyl meltdown in 1986, have revealed flaws and gaps in disaster preparedness. The region around the reactor remains uninhabited to this day.**

*Photo courtesy of Elena Filatova; graphic courtesy of CACI*



# 2 Are Surprise and Deception Preventable?



The long history and frequent occurrence of surprise and deception emphasize that these are fundamentally psychological phenomena. Simply put, surprise, denial, and deception are effective because they challenge the perceptions that fill the very large gap between what is known and unknown. Surprise, denial, and deception also exploit natural human proclivities and inherent, systemic vulnerabilities, capitalizing on complacency, vanity, and self-delusion. There is also the proposition that strong, secure, confident nations lack the natural incentive to employ surprise, denial, and deception – often dismissed as “weapons of the weak.”

Surprise, denial, and deception have at least three shared characteristics. First, they are traumatic to the victim. For the target, surprise is an event – sudden, stunning, distressing, and even humiliating. Surprise catches victims at their weakest, exposing and exploiting their failings. The after-shocks linger on in a victim’s memory, shaping and impacting future behaviors.

**“The biggest shortcoming that we have in avoiding deception and surprise lies in the six inches between our two ears.”**

Second, they accord a significant, albeit temporary, advantage to the initiator. For the initiator, surprise is a process, or more precisely, an outcome

of a deliberate, often painstaking effort. It is a plan coming together in a concentrated burst of activity in which everything worked just right to produce the expected result. Having achieved surprise, the initiator sets out on a mission to exploit the initial success so as to achieve the desired political, military, economic, or informational objectives.

Finally, surprises generate a seemingly endless stream of analyses and second-guessing. Scrambling to recover, the target tries to determine what happened and why; who was at fault; and how to reorganize the “system” in order to avoid a similar failure in the future. It is only after the fact that the victim becomes aware of what caused the event to happen. In other words, the target learns the makings of a surprise only in retrospect. The task of “connecting the dots,” even noticing that there are dots, signals, and indicators out there, is quite simple once one knows what to look for. Therefore, in retrospect, one tends to be less impressed by the initiator’s skill than

by what appears to be the victim’s own fatal self-delusion, if not abject blindness.

By definition, what makes surprise happen is the unbelievable, unpredictable act that one group or nation cannot conceive – but that another one can. The more ingrained and widely held the assumptions as to whether an event could happen – the when, where, by whom, and how it might be carried out – the greater the cognitive dissonance when expectations are shattered by a suddenly altered reality. By the same token, the stronger the going-in assumptions, the more rigid the processes, and the more valuable the information that has been lost along the way – the higher the potential for cognitive dissonance, and consequently, the more persistent the operational paralysis.

The greater the surprise, the more important time becomes as the critical factor in the target’s ability to adapt, regain footing, and adjust to the new reality.

**Surprise, denial, and deception are effective because they challenge the perceptions that fill the gap between what is known and unknown.**

*Photo courtesy of CACI*



This process explains why some actors manage to recover and prevail in the aftermath of a devastating surprise, while others are left with little choice but to accept defeat. This is why it is important to understand that surprise determines the time, place, and nature of the first engagement. It rarely defines the ultimate outcome. However, this principle is precarious and must be reaffirmed each time, by both the target and the initiator.

Harbor and thereby lost the war.”<sup>2</sup>

Japan’s faulty assumptions and misperceptions exemplify the importance of empathy in surprise, denial, and deception activities. According to one Symposium Six participant, “You need to really understand your adversary and think through their culture and thought processes. Then, once you understand what it is that they absolutely are not

difficulties and uncertainties facing both the actor contemplating a surprise and its intended target. If surprise is the result of failure to perceive, heed, or issue advance indicators of a looming threat, then warning is the antithesis of surprise, even an effective antidote to it. Furthermore, if forewarned means forearmed, warning should help avert surprise.

However, “should” is the operative word. People and organizations process incoming information through a perceptual prism, comprised of their culture, assumptions, biases, and experiences, with the most recent being the most vivid, and thus, most impactful. This prism determines which data will even be noticed and factored in and which inputs will be filtered out or ignored altogether; what weight and importance each piece of data will be accorded; which patterns the information will be arrayed into; and, ultimately, which judgments and conclusions will be derived. “We tend to revert to our intuitive thinking, even when it’s not appropriate for the kind of situation we are in,” said one participant. “Therefore, we have a tendency to dismiss important information that otherwise might cause us to think or to decide differently.”

Within this natural, if rarely explicitly recognized, process, there are specific points of vulnerability where new, often critical, information is filtered out, dismissed as irrelevant, ignored, or simply left out. Insofar as the perceptual prism is dynamic and new facets are formed every time input is sorted into the patterns that constitute memory, such information becomes, effectively, irretrievable. This goes a long way toward explaining why collecting vast amounts of data does not necessarily lead to better situational awareness and decision superiority. It also explains the tendency to repeat past



### **The USS Arizona (BB-39) burning after the Japanese attack on Pearl Harbor, December 7, 1941.**

*Photo courtesy of National Archives and Records Administration*

Being a target does not automatically make one a victim. The impact of the initial shock might be short-lived; the advantage is fleeting. The target, if capable and resolute, is just as likely to recover and respond – at times in an asymmetric, if not disproportionate, manner, imposing a price far exceeding the initiator’s original cost-benefit calculus. A prime example is the attack on Pearl Harbor. The Japanese believed this would prevent the U.S. Pacific Fleet from interfering with Tokyo’s political, economic, and military designs in Southeast and Northeast Asia. Not only were the Japanese thoroughly mistaken about America’s intentions, they brought the U.S. directly into World War II. Japanese Admiral Hara Tadaichi, who commanded Japan’s Carrier Division 5 in the attacks, quickly concluded that “the attack did not fit any thinking that I knew to be right ... We won a great tactical victory at Pearl

going to do – the cultural and religious barriers they say they are not going to cross – you plan for that to happen.”

The tendency in most planning is to confuse the unfamiliar with the improbable. The unconsidered contingency looks strange, and therefore, unlikely. What is improbable need not be considered seriously.

To avoid the distortion of hindsight typical of any ex post facto analysis, national security actors must view situations as if they were in their adversaries’ shoes and actual scenarios were unfolding. “We need to try to find a way to develop this attribute of empathy, the ability to look at things through other people’s eyes,” said a Symposium Six participant. This is essential to being able to recognize and learn from the

<sup>2</sup> Herve Haufler, *Codebreaker’s Victory: How the Allied Cryptographers Won World War II* (New York: NAL, 2003), p.127.

errors and why recording lessons is so fundamentally different from actually learning from the experience.

---

**"If everything is crystal clear, the adversary behaves just like you would in similar circumstances, and everything seems consistent with your best-case scenario, you are probably being deceived."**

---

The issue of warning is at the juncture of intelligence, strategy, operations, and decision-making writ large. At its most basic, warning is information pointing to the emergence of an acute threat to a nation's security. That information is obtained and processed by the intelligence agencies and transmitted to decision-makers for action. Warning, therefore, is the vital link connecting intelligence assessment with countermeasures and other preparations designed to face a looming threat.

Indications and warnings are collected, processed, evaluated, analyzed, and disseminated by the C4ISR community, a highly complex, largely closed system comprising individuals, groups, organizations,

technologies, and processes. The people who make up the system are subject to biases, preconceptions, and a wide range of human factors that shape their perceptual prism – the mental lens through which each absorbs and processes information. As data and inputs that could become warnings circulate through the system, they are subject to interpretation, reinterpretation, and modification by the dynamics of these diverse groups and hierarchies. The path that a potential warning takes affects its timeliness, content, detail, and level of urgency. Ultimately, a warning should reach a decision-maker for action.

Warning means nothing if decision-makers fail to act in a timely manner. Such failure might occur for any number of reasons, ranging from reluctance to question the authority of conventional wisdom; through the often-justifiable concern that overt counter-measures and other steps to enhance one's readiness might actually be mistaken as aggressive and provoke the adversary; to the basic inability to imagine the nature and magnitude of a looming threat and the ensuing necessity to act promptly.

Successful denial and deception, as well as timely warning and decision, hinge on an accurate understanding of the capabilities and limitations of C4ISR. If collection and analysis sources, methods, and processes are known, an adversary might be able to avoid or delay detection, thus buying time and enhancing the chances of achieving surprise. Likewise, if an adversary's sources of information and decision-making processes are well understood, there is a good chance it can be manipulated by controlling the flow of information, adding misleading information, and distorting an opponent's perceptions.

The effectiveness of surprise, denial, and deception are rooted in the imperfection of human nature, and therefore, inherent in the very nature of force and diplomacy. For the U.S. and other countries alike, strong capabilities in C4ISR, data management, and the full range of government and societal information systems can only ameliorate – but not eradicate – incidences and consequences of surprise, denial, and deception. The challenge, then, is how well these risks can be mitigated.

**C4ISR centers leverage the full range of government and public information, and may reduce, but not eradicate, the incidences and consequences of surprise, denial, and deception.**

*Photo courtesy of Joint Air Defense Command*





# 3 Leadership, Authorities, and Decision-Making

The challenges of surprise, denial, and deception go far beyond perception, intelligence, and warning. The institutions and processes designed to deal with these threats are not necessarily equipped to handle them. According to one Symposium Six participant, “The speed of information is overwhelming every system that we have. First, the Intelligence Community is going to need to be smaller and leaner, and therefore has to be agile in a war ... It has to be very flexible. And it has to possess deployable capabilities, people, processes, and systems, and remain technologically advanced, slightly ahead of our adversaries, while retaining our cutting edge against those most challenging, difficult adversaries that we face.”

Looking to additional interagency capacity in the information age, the U.S. government must capitalize on information, not in a special operations manner, but in an above-board, cohesive manner to contribute to achieving our national security objectives.

However, as one Symposium Six participant stated, “There’s incredible complexity in the globe. And this uncertainty in our interagency process is not ineffective, but it is very inefficient because there are people, organizations, commanders, and authorities that have that fingertip feel for what is going on in their environment ... [who] feel they don’t have any authority to be able to make a decision because everything has got to be choked inside of this thing we call the interagency process.”

---

**“If the U.S. is to have decision superiority in countering asymmetric threats, it needs the leadership, authorities, and decision-making processes and structure to enable this superiority – and in working to this end the United States faces a daunting challenge.”**

---

If bureaucracy has a chokehold on decision-makers, then outdated national

security policies have tied their hands. The United States continuously faces asymmetric threats and devises countermeasures to them. Competitors have adapted to these countermeasures better and more rapidly than new countermeasures can be devised. “You can’t fight asymmetric threats with plans and strategies and – even more important – policies that are so wrapped up in symmetry that those who have got to do the work aren’t able to be nimble and flexible enough to defeat the threat.”

Placing the challenge in a broader context is the U.S.’s sizable national debt. The looming budget sequestration requirements of 2013 threatens far deeper cuts in the defense budget. As one participant noted, “In the past, we had the luxury of unlimited resources, so we adopted a brute-force approach that focused on effectiveness and not efficiency. Just throw things at the problem because we’re trying to figure it out as we go. [But] we have never had multi-trillion-dollar debts ... so we can no longer use that model.”



**Those dealing with asymmetric threats have to plan and execute while facing America's sizable national debt and the looming threat of sequestration in 2013.**

*Image adapted from a photo courtesy of Johan Frøhman*

For the U.S. to maintain world leadership in military technology, new focus should be brought to bear on challenges to leadership, authorities, and decision-making in four areas: (1) biochemical capabilities, (2) cyberspace, (3) educational institutions, and (4) interagency cooperation.

Consider biological warfare defense and public health issues. The appropriate services and agencies are collaborating on biological and chemical defense issues, but “the challenge is not so much having the right players in the room, but having

U.S. public health and national security authorities, meanwhile, may not be prepared to prevent or fend off a large-scale viral infection or biological attack. Prior to the H1N1 pandemic in 2009, there was significant public-private investment with industry subsidies to expand vaccine capacity. Today, however, the U.S. still looks to foreign suppliers for influenza vaccines. The major expenditures involved to protect against mass infection or attack are also part of the problem. “The state of public health in the United States has fallen on hard times in the current economic crisis,

A large part of the challenge comes from the fact that the private sector owns over 85 percent of the nation’s critical infrastructure. The government does not have the capability and capacity to operate alone in this environment. In turn, the private sector is worried about liability and how much information needs to be shared. Such uncertainties lead to reactive and piecemeal solutions to evolving threats. In the cyber world, said one participant, “all too often, we find tactical successes to be really fulfilling, and then discover the real problem did not go away.”

**President Barack Obama being briefed about the 2009 H1N1 swine flu outbreak by administration officials.**

*Photo courtesy of the Executive Office of the President of the United States*



them understand issues that are totally alien to them.” What is needed is “a common understanding of the evolving language, principles, and operations of national security since 9/11.”

Throughout the 1950s and 1960s, the U.S. had a second-to-none strategic advantage over the Soviet Union with strategic, operational, and tactical biological weapons. Under President Nixon, the nation renounced that capability for well-founded reasons, but others did not choose the same path. China, India, North Korea, and many others invested in biotechnology capabilities, including many legitimate investments to bolster food supplies and serve healthcare needs. However, their ongoing development could also set the stage for biochemical surprise.

which goes beyond the federal level to the states,” said a Symposium Six participant with healthcare expertise. “At least 35 states have such economic problems that they are literally thinning the public health workforce.” Looking to the future, there are no adequate mechanisms to distribute vaccines or administer them to first responders or the general population. Without such a mechanism, biological attacks can cause significant economic impacts and social disruption.

There also are significant challenges in defending the nation’s critical infrastructure from cyber attack. Cyber attacks are unique in that they can be individual acts, force-multipliers, or precursors of other attacks. Part of what makes a small cyber attack so troubling is the potential for an exponentially larger impact.

Modern communications present another cyber challenge. Following Operation Desert Storm, the Air Force decided to place more emphasis on command and control and to create robust combined air operations centers for planning at the combatant commands. This was a highly successful strategy for its time.

Twenty years later, in a world of distributed technologies where adversaries can quickly negate such a center’s communications processes, there is a need to evolve to a more distributed ability to plan and execute operations.

Finally, it may be necessary to take a more ambitious step and re-examine the entire interagency process.



Current interagency processes are an outgrowth of World War II and the National Security Act of 1947 – a far different world from the second decade of the 21<sup>st</sup> century. “It is not a matter of redesigning the interagency process,” according to one participant. “It needs to be blown up and started over again with a clearer understanding of the rapidity with which actions occur. And this new architecture needs to take into consideration that the military will not always be the solution.” There have been various reorganization boards, commissions, and panels over the years, but significant reorganization must be driven by Congress.

Simply reorganizing the national security decision-making infrastructure may not be enough. According to another Symposium Six participant, “I’m not sure you can reorganize the Intelligence Community to

institutionalize responsibility for precluding surprise and deception. I think to some extent this is a cultural thing. And the more you have given somebody the responsibility for it, the more likely it is that everybody else doesn’t talk the culture or practice it.”

There are examples, however, that such a cultural shift is not only possible, but already working well. The interagency collaboration in the National Cyber Investigative Joint Task Force, led by the FBI, is one such example. This effort has 20 departments and agencies working daily, integrating, coordinating, and sharing information on the threat side of cyber investigations. “We have numerous successes where we can see, end-to-end, one agency bringing in an issue, handing it off to another agency, and then the issue wraps back around with a successful outcome,” said one participant. The key is collaboration

rather than mere information sharing as the end goal.

Federal agencies are also working effectively with the private sector, as exemplified by the work of the National Cyber-Forensics & Training Alliance in Pittsburgh. The FBI is a partner with private-sector companies in developing cyber strategies. The federal partners get involved when the issue becomes transnational and involves law enforcement. The only challenge with these interagency successes is funding these initiatives out of existing agency budgets.

To say that surprise, denial, and deception challenge national security capabilities and authorities is an understatement. Yet the awareness of these issues and the innovative ways these challenges are being addressed show that the U.S.’s ability to adapt should not be underestimated.



**Current interagency processes are an outgrowth of World War II and the National Security Act of 1947 – a far different world from the second decade of the 21<sup>st</sup> century.**

**President Harry S. Truman at his desk in the Oval Office, signing the National Security Act Amendments of 1949.**

*Photo courtesy of Harry S. Truman Library*



# 4 Strategic Implications



History is replete with examples of countries (and their militaries) that failed due to their inability to transform organizations and culture, adopt new operational concepts, or leverage breakthrough technologies. Failure occurs in the context of an overall national debacle caused by systemic problems that fall into three distinct but related categories.

First is the failure to *anticipate* the nature of and trends within the strategic environment; the character and resilience of the opponent; a nation's own will and resolve; the impact of technology – be it new or old but used in new ways; and perhaps most importantly, failure to anticipate the second- and third-order consequences of both action and inaction.

Second is the failure to *learn* from experience – of both the U.S. and others. Selective reading of history – especially coupled with faulty analysis – is particularly pernicious here, as is mistaking “lessons recorded” with lessons actually learned.

Third is the failure to *adapt* behaviors, concepts, and institutional constructs to the ever-changing domestic and international dynamics, as well as evolving adversarial operational, tactical, technological, and/or doctrinal innovations. Failure to validate pivotal assumptions and adjust accordingly falls in this category as well. In contrast to these shortcomings, victory – and hopefully long-term security – comes to

those who foresee, recognize, and act on changes emerging in the strategic global environment.

---

**“Today's confluence of global trends foreshadows significant challenges to U.S. organizations, systems, concepts, and doctrines. The nation is at an historic turning point demanding an equally comprehensive revolution.”**

---

The U.S. must balance current exigencies with future requirements. Any single-focus approach bears a huge opportunity cost. The rest of the world has not taken a time out while America tended to Iraq, Afghanistan, and other issues. The U.S. must beware of complacency and the perils of strategic myopia. Operational concepts and institutional structures, valid for a specific time and place, should not be allowed to become dogma, stifling fresh thought. That, too, is a prescription for failure.

The future strategic environment will be shaped by the interaction of globalization, economic disparities, and competition for resources; diffusion of technology and information networks whose very nature allows unprecedented ability to harm and potentially paralyze advanced nations; and systemic upheavals impacting state and non-state actors, and thereby international institutions and the world order.

The following are salient features of this increasingly complex, dynamic, lethal, and uncertain environment:

- Violent extremism and ethnic strife – a global, generational, ideological struggle;
- Proliferation of weapons of mass destruction and empowering technologies;
- Rising peer competitors with voracious appetites for resources and influence;
- Predatory and unpredictable regional actors;
- Increasing lethality and risk of intrusion by terrorist and criminal organizations;
- Systemic instability in key regions (political, economic, social, and ideological);
- Unprecedented velocity of technological change and military adaptation;
- Availability of advanced weapons in a burgeoning global marketplace;
- Exponential growth in volume, exchange, and access to information;
- Greatly reduced ability to retain high-level national security secrets, political, operational, or technological;
- Extremely rapid decay rates for any domain advantage;
- Surging globalization, interconnectivity and competition for scarce resources; and
- Dislocating climate, environmental, and demographic trends.



The U.S. and its allies face threats ranging from existential to potentially crippling perils. At the high end are existential threats that have extreme capability but low intent; at the low end are terrorist attacks like 9/11, with low capability but very high intent. The U.S. must pay close attention to everything spanning that range.

*Pentagon photo courtesy of the U.S. Air Force*

These global dynamics are closely intertwined with the changing character of 21<sup>st</sup> century warfare. Having experienced or vicariously learned the cost of challenging the U.S. head-on, would-be adversaries are developing asymmetric approaches to attack vital levers of U.S. power. They find maneuver space and sanctuary in dense urban areas, ungoverned hinterlands, and loosely regulated information and social networks. Their strategies seek to circumvent core U.S. advantages, while undermining international support and domestic resolve.

**"Terrorists have surprised us. Regional instability has surprised us. Who could have predicted that a Tunisian vendor setting himself on fire would have kicked off what has kicked off over the last year or so?"**

Meanwhile, ascendant powers – flush with new wealth and hungry for resources and status – are posturing to contest U.S. superiority. These adaptive competitors are also translating lessons from recent conflicts into new

concepts, capabilities, and doctrines tailored to counter U.S. strengths and exploit vulnerabilities. These include:

- Anti-access area-denial weapons and operational concepts designed to limit U.S. freedom of action, which could place carrier battle groups and amphibious forces at unacceptable risk;
- "Generation 4-plus" aircraft<sup>3</sup> that could challenge America's existing inventory and, potentially, air superiority;
- Increasingly lethal, integrated air defense systems that could negate weapons and tactics used to suppress or destroy these systems;
- Proliferation of surface-to-surface missiles with growing range, precision, mobility, and maneuverability, which would be capable of delivering both conventional and non-conventional payloads;
- Proliferation of unmanned aerial systems capable of conducting low observable, persistent,

intrusive missions in both lethal and non-lethal modes;

- Resurgence of offensive counter-space capabilities;
- Increasing ability of even marginal actors to observe the disposition of U.S. assets through widely available, inexpensive commercial means; and
- Attacks through cyberspace that are already creating adverse tactical, operational, and strategic effects at low cost and with relative impunity.

Among existential threats to the U.S. are:

- Large-scale nuclear attack;
- Biological attack against people and/or food and water supply;
- Total cutoff of energy;
- Massive cyber attack – including electromagnetic pulse (EMP) weapons<sup>4</sup> – which would bring U.S. services and the economy to a standstill;
- Rapidly spreading pandemic overwhelming all services;
- Natural disaster on an unimaginable scale; and
- Weaponized, disruptive technology that threatens extinction or long-term paralyzing disruptions (e.g., bio-engineering, plasma weapons, etc.).

Among existential threats to allies – possible but highly unlikely to the U.S. – are:

- Foreign invasion;
- Genocide;
- Violent overthrow of the government, resulting in a civil or cross-border war;

3 Fourth-generation aircraft include multi-role fighters equipped with increasingly sophisticated avionics and weapon systems, also emphasizing maneuverability rather than speed. Fifth-generation fighters use advanced integrated avionics systems to provide

complete battlespace awareness, and use low observable "stealth" technology. Examples include China's J-20 and Russia's T-50 fighters. GlobalSecurity.org at <http://www.globalsecurity.org/military/world/fighter-aircraft-gen-1.htm>.

4 A weapon that produces a powerful electromagnetic field within the vicinity of the weapon burst capable of causing irreversible damage to a wide range of electrical and electronic equipment, particularly computers and radio or radar receivers. GlobalSecurity.org at <http://www.globalsecurity.org/military/library/report/1996/apjemp.htm>.

- Famine (natural or man-made); and
- Climate change leading to mass migration.

Existential threats to the U.S. must also be distinguished from crippling threats that could severely affect either a segment of society, a geographic region (e.g., massive earthquakes on the West Coast), or an isolated portion of the country's infrastructure. A crippling threat is reversible, although the recovery could be long and painful. A synchronized series of crippling threats might become existential, if the U.S. fails to regain decision superiority, respond properly, and break the chain of cascading effects. The list of possible crippling threats is much longer and includes:

- Localized radiological explosions (dirty bomb);
- Threat to essential commodities such as water, fuel, food, medicine, etc.;
- Geographically isolated natural disasters;
- Isolatable low-order nuclear, chemical, or biological attack;
- Large-scale refugee flow into southeast or southwest U.S.;
- Blockage or incapacitation of major transportation nodes;
- Sporadic cyber attacks on communication infrastructure, stock exchange, power grid, water supply, etc.;
- Synchronized terror attacks on high-value, high-prestige targets;
- Massive public unrest resulting from some or all of the above; and
- Economic collapse.

Additionally, there are asymmetric threats that are more recognizable to the general public, such as:

- Threats to aviation – Since 9/11, there have been over 40 hijacking attempts, with one of those being attempted for terrorism purposes;
- Threats to mass transit – There are about 250 attacks per year worldwide; and
- Lone offenders, copycats, and individual fanatics.

In the 20<sup>th</sup> century, the U.S. and its allies were alarmed by nation states that were too strong – twice Germany, once Japan, and for a long time the Soviet Union. In this century, what should alarm the U.S. is that some nation states are too weak. Pakistan may be a prime example, afflicted by

is worldwide. It is unlikely that the effectiveness of surprise, denial, and deception activities will abate any time soon. Therefore, the U.S. is bound to confront such schemes wherever it engages to promote and defend its interests. The U.S. must be vigilant of adversaries' breakthroughs in fields such as cybernetics, nanotechnology, biotechnology, electromagnetic spectrum physics, robotics, advanced propulsion, etc. It cannot be assumed that the next military revolution will originate in the West. Indeed, the hub of innovation in science and engineering education has shifted eastward. Therefore, the U.S. must anticipate innovative combinations of traditional

**The U.S. should expect to be asymmetrically challenged in all domains, including space and cyberspace, as well as on land, at sea, and in the air.**

*Graphic courtesy of CACI*



a number of insurgencies, some of which it sponsors, at least informally as a matter of policy by instruments of the state; it is a nation state with not just a large nuclear weapon store but the most rapidly growing nuclear weapon store in the world – the world's number one proliferation threat. Perhaps a far more terrifying scenario than Iran's acquiring nuclear weapons is that of Pakistan losing control of some of its nuclear weapons.

Even if the U.S. continues to successfully dissuade and deter major adversaries, their advanced technology proliferation

and new concepts, doctrines, weapons systems, and disruptive technologies.

These global dynamics have put the U.S. and global security at a strategic crossroads. From this point forward, the U.S. should expect to be asymmetrically challenged in all domains, including space and cyberspace, as well as on land, at sea, and in the air. Perhaps for the first time in history, the ability to inflict damage and cause strategic dislocation is no longer directly proportional to capital investment, superior motivation and training, or technological prowess.



# 5 National Imperatives Moving Forward

The ancient war story of the Trojan horse is a legendary tale of surprise, denial, and deception. After a 10-year siege of the city of Troy, the Greeks built a large wooden horse, hid some 30 soldiers inside, and left it in front of the city's gates. When the Greeks pretended to sail away in defeat, the Trojans pulled the horse inside as a victory trophy. As the Trojans slept, the Greeks emerged from the horse and let the rest of their army into the city.

Troy was destroyed and the Greeks decisively won the war. Although these events took place around 12<sup>th</sup> century BC, the use of surprise, denial, and deception are as prominent as ever. Even today, a *Trojan horse* is a name given to deceptive malware that infects computer programs.

While surprise, denial, and deception cannot be eliminated, they can be mitigated. The effectiveness of these efforts depends on whether national (and global) security players and institutions can evolve with – or beyond – the threats.

---

**"The only thing that shouldn't surprise us is that there are still some things out there that can surprise us."**

---

American national security leaders have the opportunity to make the innovative changes necessary to move forward.

## Cultivate

If surprise, denial, and deception are the results of gaps in perception, then the logical conclusion is to improve how national security actors see things. Existing perspectives and paradigms still rest heavily on symmetric thinking. "Our intelligence workforce has to be conscious and be ready because we are not going to be predictive," said a Symposium Six participant. "To think that we can be clairvoyant or predictive is foolish."

In that case, there is a clear need to cultivate better ways of thinking,

from observation to assessment. As another participant explained, "First, we need to understand more about *how* we think, and we need to be introspective enough ... to identify what method is appropriate and then try to use it. We have to deliberately choose to use analytical methods and not revert to our natural tendency to be intuitive." Intuition is still an important part of the intelligence process. Perception gaps, however, are often gaps in experience and exposure – both of which form intuition.

Changes to national security thinking also require the ability to perceive situations as others do. "We need to find a way to develop empathy, the ability to look at things through other people's eyes," said one participant, noting that this is a skill that seems to be diminishing in our increasingly polarized world. "It is often not the availability of information that we have," said this individual, "but our method of thinking that leads us to be surprised."



**The Trojan horse, as depicted on a Corinthian aryballos, ca. 6<sup>th</sup> Century, BC.**

*Reproduction courtesy of Kaiserlich Deutsches Archäologisches Institut*

Empathy may help better understand adversaries and other actors, but it is only part of the equation. According to one participant, “I talk to Chinese subject matter experts, and they tell me about what is going on in the South China Sea. My first question is: what is going on in South America? What is going on in Central America? What is going on in Africa? If they don’t have those answers, they’re not subject matter experts on what the Chinese are doing. We have to have people that are thinking a little bit beyond just their little scope of the world.”

During the Cold War, the worldwide interests of the Soviet Union and their communist sphere of influence were a constant concern, most notably culminating in the Cuban Missile Crisis. Such breadth and depth of thinking, informed by cultural awareness, is critical in addressing globalized security challenges.

### **“There are no universal standards of rationality – or stupidity!”**

Cultivating better ways of thinking about national security also means creating a culture in which different insights and ideas are seriously considered and incorporated. One Symposium Six participant put it quite clearly:

“We need to encourage our mavericks, create environments where dissenting opinions are valued. The best decision-makers I have ever known have valued people from a variety of backgrounds, and they encouraged dissenting views to be voiced.”

Decision-makers do not always have to agree with dissenters, but must be willing to hear different opinions and be open to changing their minds. They must not be “drowned out by folks who already knew what the answer was” before they sought advice.

While national security leaders should set the example of considering multiple viewpoints, it is essential that this change in thinking take place throughout national security organizations. The U.S. must develop a cooperative relationship with all those who might provide new insights and different perspectives. As one participant stated, “Keep this circle as diverse and wide as practicable and help your colleagues by asking the ‘right’ questions – tell them

### **Perception gaps are critical to addressing globalized security challenges such as the Cuban Missile Crisis.**

**A U.S. Navy patrol aircraft over a Soviet freighter during the Cuban Missile Crisis, December 5, 1962.**

*Photo courtesy of the U.S. Navy*



does not necessarily translate into improved warnings. “Don’t assume or expect that appropriate decisions, authorities, and actions would automatically follow warning,” said one Symposium Six participant. Taking action against surprise, denial, and deception tomorrow means investing in capabilities today.

Shaping future national security capabilities will certainly be demanding. According to another participant,

explicitly what you need to know and why. But be realistic: we are yet to develop C4ISR systems that can assess intentions. Question the bona fides of any information – no matter how comforting, consistent, convincing, or highly classified.”

Changing thought processes and considering different perspectives can sometimes be awkward and uncomfortable. However, resorting to old ways and refusing to evolve will simply cultivate more problems.

## **Invest**

Improving the national security system may begin with changing how issues and adversaries are understood, but it will require changing how the system operates. Better intelligence

“First, the Intelligence Community is going to need to be smaller and leaner. It’s about this idea of agility, adaptability to a degree, but agility. It has to be very flexible. It has to have an expeditionary mindset, just like we have asked our forces to have. And it has to possess deployable capabilities – people, processes, and systems – and remain technologically advanced, slightly ahead of our adversaries, while retaining our cutting edge against those most challenging, difficult adversaries that we face.”

The first step is always reassessing priorities and resource allocation. “We need to consider what our global posture needs to be. Where do we put things? Where do we have people?”

One of the costliest mistakes national security planners can make, according to





**Tahrir Square in Cairo, Egypt on February 8, 2011. Events like the “Arab Spring” show how quickly things can change.**

*Photo courtesy Mona Sosh*

one participant, is “fall[ing] in love with [their] plan, policy, program, or assessment.” The difficulty of developing strategies and obtaining resources and buy-in can lead to one-size-fits-all approaches to a country or specific issue. It is not common for national security priorities to shift overnight. However, events like the “Arab Spring” show how quickly things can change. Resistance to change could only handcuff decision-makers and cause misallocation of resources. “State your planning assumptions up front, clearly and explicitly. Identify pivotal assumptions – those that, if proven wrong, would upend your entire approach. Develop a system to periodically revalidate these assumptions, making sure you don’t confuse estimates with facts, or hopes with viable courses of action.”

---

### **“Don’t get complacent. Hubris kills.”**

---

Creating a leaner national security community will also be a difficult, but necessary step. “Where we require a more robust presence, emphasizing and prioritizing, where we believe potential problems are likely to occur, we have to consider legacy platforms that should remain,” a participant stated. “We have to decide which ones should be retained. And we’re going to have to make some hard decisions about which ones should

be eliminated. That includes some of the talent that comes with that. We have contracted a huge contracted workforce, an enormous amount of talent. We’re going to have to figure out how we adjust our security needs based on what we lose there – because we are going to lose.” As unpalatable as across-the-board budget cuts would be, the threat of sequestration may be a motivation to instill fiscal discipline according to what national security agencies will and will not need going forward.

In an era of doing more with less, it will be more important than ever to fully capitalize on past investments. “We have to protect the investments that we have made in our people,” a participant said, noting the importance of prioritizing critical investments in technology and new capabilities, “especially in cyber and ISR [intelligence, surveillance, and reconnaissance] systems, and some of the processes we have foxhole to space, especially in the exploitation realm.”<sup>5</sup> This is essential, especially if national security leaders want to preserve the ability to change course and make program changes. According to another participant, “We acknowledge the need for reversibility: reversibility in people, which is not as easy as it sounds;

reversibility in the industrial base, which is even harder; and, again, to avoid that departmental hubris.”

Empowerment is particularly applicable to information superiority. Throughout history, leaders at all levels have operated with limited information and constrained situational awareness. With advances in sensors, information sharing, and network-centric systems, decision-makers are suffering the embarrassment of riches – they are, quite literally, struggling with information delivered at a velocity and volume far exceeding their ability to absorb. The U.S. must develop and field systems that are not just network-centric, but knowledge-centric. These systems would process and integrate data in a manner consistent with natural neurological patterns, presenting information in a format that enables timely, logical decisions. Such self-forming, self-healing networks that fully harness the power of machine-to-machine interface would free up human resources for activities where intellect and spirit remain indispensable.

Investing in national and global security capabilities is often mistaken for large financial outlays. Yet improving how priorities are defined and resources are used may be the more valuable use of time and energy to counter surprise, denial, and deception.

---

5 One idea of investing in talent is doing a better job of retaining math, science, and engineering graduates, many of whom return to their home countries or head to the private sector after obtaining advanced degrees.



## Leverage

Some of the most important national security resources a country can have are its relationships across government, with foreign nations, and with the private sector. The complexities of surprise, denial, and deception require leveraging partnerships with those who have complementary resources and who also suffer the consequences of such threats. To mitigate the risk, the U.S. must retain a modern, agile, and well-trained military; responsive, collaborative cooperation among government agencies; and a responsible, engaged private sector. It also needs to evolve new deterrence concepts. As one participant said, “In particular, the U.S. must to rethink notions such as extended deterrence and conceive new ways of dealing with asymmetric actors who might have been deemed ‘undeterrable’ in the Cold War construct.”

While task forces and working groups across government are nothing new, they have been typically narrow in scope, with limited authority, and short-lived. It is clear that interagency cooperation will have to overcome many organizational and cultural obstacles to fully exploit the knowledge, skills, and insights that already exist. However, according to another Symposium Six participant, “One of the good news stories ... is how the Intelligence Community in this country, along with other agencies, has come together in the wake of 9/11 to protect this country.”

International cooperation is also not a new concept. Military and strategic alliances are as old as nation-states themselves. Certainly with its closest partners in the world, the U.S. is to a very large degree sharing intelligence and operational information.

---

**“If we don't have secure, confident, and reliable partners ... we can't preserve our own interests as well.”**

---

However, in today's asymmetric threat environment, international partnerships will have to not only be more innovative, but also include regions where close relationships have not traditionally existed before. “We can't afford to do it the way we used to do it,” a participant emphasized, “and there's no going back. We have to expand on existing alliances and build new and innovative partnerships that strengthen alliances, especially in places like Africa and Latin America.” This is especially important with the U.S.'s strategic shift towards the Pacific and staying up to speed in areas of interest to China.

As strategic interests and challenges evolve, national security leaders will have to increasingly engage the private sector. The private sector has always been seen as a source of innovation, where public-private partnerships have traditionally focused. However, owning more than

85 percent of American infrastructure, corporations have found themselves on the front lines as targets of surprise, denial, and deception activities, particularly in cyberspace. Likewise, the private sector is also a key partner with the government in absorbing, rebuilding, and reconstituting capabilities from such multi-faceted asymmetric attacks.

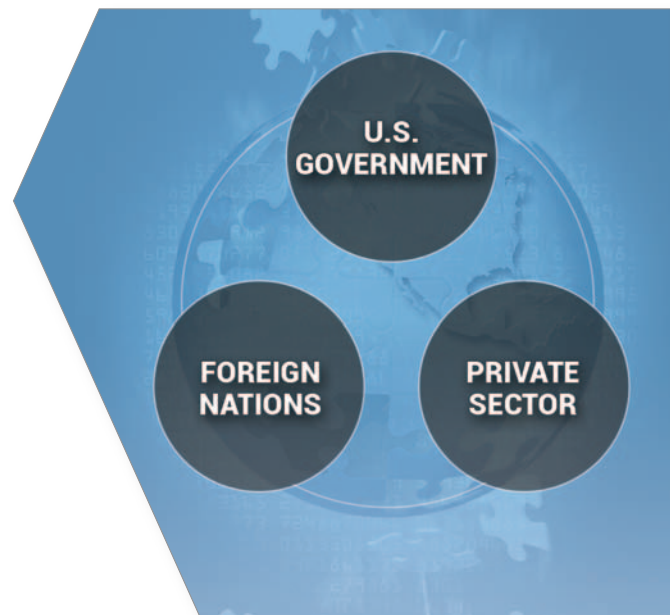
Leveraging the benefits of partnerships is more important than ever. “The bad guys are coming together,” one participant said. “Terrorists and leaders of very powerful drug trafficking cartels ... At the same time, we're floating further apart.”

From sharing intelligence to joint operations, relationships with partners across agencies, borders, and sectors are essential in mitigating surprise, denial, and deception threats. “Partnerships will matter more this century than they did in the last few centuries,” a participant stated. The U.S. must extend its values, ideas, and ideals about why nations must work together in our globally interdependent world.

---

**Some of the most important national security resources a country can have are its relationships across government, with foreign nations, and with the private sector.**

*Graphic courtesy of CACI*



# 6 Conclusion

As the Chinese general Sun Tzu wrote, “All warfare is based on deception.” Surprise, denial, and deception may be some of the oldest tricks in the book. Yet history shows us these are tricks that are fallen for over and over again. The symposium on *Decision Superiority: Countering Surprise, Denial, and Deception* was held to contribute to the national discourse on how these threats may be countered in the current security environment.

It is clear that these threats cannot be eliminated. Not only will surprise, denial, and deception continue to exist because of gaps in our abilities to perceive them, they are also far too effective to not use.

“You are not going to prevent deception and surprise. It is what the bad guys do.”

It is up to national and global security leaders to overcome organizational and cultural hindrances that have created intelligence and operational gaps, and identify opportunities for improvement. Strategic risk can also mount through the accumulation of shortfalls in recapitalization and modernization, obsolete strategic and operational concepts, failure to revitalize organizational ethos, and unwillingness to let go of outdated structures, bureaucratic arrangements, sector boundaries, and hierarchical relationships. America’s global posture

and future success depend upon the ability of its people and organizations to adopt new, relevant concepts, constructs and technologies, suitable to the dynamics of the strategic environment.

As the combination of information superiority and decisive action, decision superiority will be achieved by better understanding today’s threats, improving resilience, and better integrating the perspectives and the players in national security. Those who don’t will be condemned to keep falling for the same old tricks of surprise, denial, and deception.



**With adversaries like China deploying advanced stealth aircraft, and countries like Iran possessing nuclear capabilities, it is more critical than ever for the U.S. to vigilantly guard against surprise, denial, and deception.**

*Graphic courtesy of CACI; map imagery ©2012 Cnes/Spot Image, DigitalGlobe, GeoEye, Map data ©2012 Google*

# Acknowledgements

## Symposium Participants

(alphabetical order)

### Michael Braun

Former SES and Chief of Operations,  
U.S. Drug Enforcement Administration;  
Managing Partner, Spectre Group International

### Michael Brown

Rear Admiral, USN (Ret); Former Director,  
Cybersecurity Coordination, U.S. Department  
of Homeland Security; Vice President  
and General Manager, RSA Federal  
Business, Security Division of EMC

### Bert Calland

Vice Admiral, USN (Ret); Executive Vice  
President for Security and Intelligence,  
CACI International Inc  
VADM Calland also served as Advisor

### Steven R. Chabinsky

Deputy Assistant Director, Cyber Division,  
Federal Bureau of Investigation

### Kevin P. Chilton

General, USAF (Ret); Former Commander,  
U.S. Strategic Command

### Paul M. Cofoni

Chief Advisor, Board of Directors, and Former  
President and CEO, CACI International Inc  
Mr. Cofoni also served as Advisor

### Peter H. Daly

Vice Admiral, USN (Ret); Chief Executive  
Officer, U.S. Naval Institute  
VADM Daly also served as Advisor

### David Deptula

Lieutenant General, USAF (Ret); Former  
Deputy Chief of Staff for Intelligence,  
Surveillance, and Reconnaissance (A2), Air  
Force Staff; Chief Executive Officer, Mav6

### Michael Flynn

Lieutenant General, USA; Director, Defense  
Intelligence Agency; Former Deputy Director,  
National Intelligence, Office of the Director of  
National Intelligence

### Frank J. Gaffney

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

### Dan Johnson

U.S. Department of Homeland Security,  
Office of Intelligence and Analysis

### Michael D. Jones

Major General, USA (Ret); Former Chief of  
Staff, U.S. Central Command; Management  
Consultant and Member, SPECTRUM Group

### Dr. Robert Kadlec

Former Special Assistant to the President  
and Senior Director for Biodefense Policy,  
White House Homeland Security Council;  
Managing Director, RPK Consulting LLC

### Dr. Lani Kass

Corporate Strategic Advisor,  
CACI International Inc

Dr. Kass also served as Advisor  
and Chief Writer

### Dr. J.P. (Jack) London

Executive Chairman and Chairman of the  
Board, and Former President and CEO,  
CACI International Inc

Dr. London is a symposia co-founder  
and also served as Advisor

### Dr. John Nagl

Professor and Minerva Research Fellow,  
U.S. Naval Academy

### James A. Winnefeld, Jr

Admiral, USN; Vice Chairman of  
the Joint Chiefs of Staff

### Jeff Wright

Senior Vice President, Enterprise Technologies  
and Services Group, CACI International Inc  
Mr. Wright also served as Advisor  
and Program Manager

## Advisors

### Dan Allen

President and Chief Executive  
Officer, CACI International Inc

### Jeff Berkin

Chief Security Officer, CACI International Inc

### Christine Brim

Chief Operating Officer,  
Center for Security Policy

### A. Denis Clift

Vice President for Planning and  
Operations, U.S. Naval Institute

### Hilary Hageman

Vice President, Legal Division,  
CACI International Inc

### Z. Selin Hur

Strategic Programs Principal,  
CACI International Inc

### Jake Jacoby

Executive Vice President, National  
Solutions Group, CACI International Inc

### Kristie Kondrotis

Executive Vice President, Business  
Development, CACI International Inc

### Ben Lerner

Vice President, Center for Security Policy

### April Parreco

Director of Conferences and Special  
Events, U.S. Naval Institute

### Dr. Warren Phillips

Professor Emeritus, University of Maryland;  
CACI Board of Directors

Dr. Phillips is also a symposia co-founder

### Dan Porter

Executive Vice President, Enterprise  
Technologies and Services Group,  
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

## Managing Editor

### Michael Pino

Publications Principal, CACI International Inc

## Graphic Design

### Chris Impink

Graphic Artist, CACI International Inc


## Art Direction

### Steve Gibson

Creative Director, CACI International Inc

*Special thanks also go to Event Manager  
Amanda Massey and Invitation Manager  
Casey Pierce of CACI International Inc.*





## NATURAL DISASTERS



## TERRORIST ATTACKS



## CYBER THREATS



**U.S. Naval Institute**  
291 Wood Road  
Annapolis, Maryland 21402  
(410) 268-6110  
[www.usni.org](http://www.usni.org)



**CACI International Inc**  
1100 North Glebe Road  
Arlington, Virginia 22201  
(703) 841-7800  
[www.caci.com](http://www.caci.com)  
[asymmetricthreat.net](http://asymmetricthreat.net)



CENTER FOR SECURITY POLICY

**Center for Security Policy**  
1901 Pennsylvania Avenue, NW, Suite 201  
Washington, DC 20006  
(202) 835-9077  
[centerforsecuritypolicy.org](http://centerforsecuritypolicy.org)