Countering Asymmetric Threats

A National Imperative

CYBER, ELECTRONIC WARFARE, AND CRITICAL INFRASTRUCTURE

STRATEGIES FOR NATIONAL SECURITY

SYMPOSIUM EIGHT

On October 1, 2014, at the Gannett Conference Center in McLean, Virginia, the Association of Old Crows (AOC), CACI International Inc (CACI), and the Center for Security Policy (CSP) co-sponsored *Cyber, Electronic Warfare, and Critical Infrastructure Strategies for National Security,* the eighth symposium in the Asymmetric Threats to National Security series.

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

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

Table of Contents

Executive Summary

On October 1, 2014, the Association of Old Crows, CACI International Inc, and the Center for Security Policy hosted "Cyber, Electronic Warfare, and Critical Infrastructure Strategies for National Security," the eighth in an annual series of symposia on asymmetric threats. The event featured a wide-ranging discussion of the threats to critical infrastructure, the role and importance of cyberspace and the electromagnetic spectrum (EMS) in both civilian life and military operations, and the steps government and industry are taking to improve the resilience of America's infrastructure, particularly the infrastructure associated with electrical power. The symposium was held under the Chatham House rule of non-attribution.

America's way of life depends on the smooth, continuous operation of a highly networked, deeply interdependent infrastructure. Beyond roads, railroads, and bridges, America's electrical grid supports every aspect of modern life, from food and potable water to hospitals and the financial system. Disruptions to that critical infrastructure, whether natural or man-made, accidental or intentional, can bring life to a standstill – or worse – and inflict billions of dollars in economic losses.

The United States has built strong institutional capacity to respond to most of the threats that the country's critical infrastructure faces. The Federal Emergency Management Agency (FEMA) and U.S. Northern Command (NORTHCOM), for example, build models and response plans for natural disasters to ensure that relief and support get to affected areas immediately after an event. But one critical area of America's way of life still lacks a unified response capacity in the event of a damaging attack or accident: cyberspace.

Cyberspace undergirds the preponderance of America's critical infrastructure: it is the network of computers, mobile devices, fiber-optic cable, and sensors that connects people, distributes information, and monitors goods as they move around the world. No nation on Earth has leveraged cyberspace and its related technologies to the extent the United States has. No other nation in recent history has used technology the way the United States has to build and maintain a preeminent military, economic, diplomatic, and political position on the world stage. Consequently, cyber technology is at once America's greatest strength and one of its biggest vulnerabilities, and America's supporting electrical infrastructure is highly susceptible to cyber threats.

Cyber systems and the EMS are also integral to American military operations. They enable vital functions, from communications to intelligence, to the command and control of forces in the field. America's military posture depends on technological superiority at every level, but the ubiquity of cyber-enabled technology and the dangers posed by its misuse or subversion mean that this superiority can no longer be taken for granted. Furthermore, although key steps have been taken to integrate cyber and EMS, such as standing up cyber commands in the services, the United States is still neither adequately prepared to counter the growing threat, nor armed with sufficiently robust capabilities.

America's adversaries – peer states, rogue states, and non-state actors – know that, for the most part, they cannot stand up to the United States military in direct combat. They must seek out alternatives to set-piece battles. The most readily available and most dangerous weapon is no longer a gun or even an improvised explosive device: it's an electron. Reliance on cyberspace and electronic communications means that nation states or rogue actors can wage cyber warfare by stealing valuable data or even diverting some of the trillions of dollars in global transactions conducted online. But the threat of cyber warfare is not limited to electronic effects. As the Stuxnet worm demonstrated, the weapons of cyber and electronic warfare can have outsized returns for a low investment, including kinetic effects that could only previously be achieved with bombs. In crafting a strategic response to cyber threats, the ability to exploit adversaries' weaknesses while compensating for America's own will be vital.

One such weakness of the United States critical infrastructure is the nation's bulk power distribution system, popularly known as the electric grid. The ready availability of electric power is essential to every other critical infrastructure sector. Without power, refrigerated food spoils, hospitals lose tools and medicine, communications systems go down. Every failure creates a cascade of second- and third-order consequences, which compound the problem. Furthermore, the electric grid, and electronic devices generally, are exposed to the unique threat of electromagnetic pulses, bursts of either natural or nuclear-generated energy that can destroy electronics and wipe out generators.

The United States has taken action to combat these types of threats to critical infrastructure, but more is required. The Department of Defense (DoD) has established cyber as the fifth domain, along with land, sea, air, and space, and the Department of Homeland Security (DHS) has created a series of responses to potential cyber threats in the form of the National Infrastructure Protection Plan (NIPP). These countermeasures, along with several Executive Orders, note the importance of cybersecurity in infrastructure protection. These actions were necessary insofar as they recognize the vital role cyberspace and the EMS play in both military and civilian life. But government activity alone will not deliver the all-threats preparedness that America requires, because the majority of the nation's critical infrastructure is owned and operated by the private sector. It will be necessary for both government and industry to work together to develop stronger security standards, improve information-sharing, and achieve better overall resilience. The price of failure is nothing less than America's way of life.

> **"Disruptions to America's critical infrastructure, whether natural or man-made, accidental or intentional, can bring life to a standstill – or worse – and inflict billions of dollars in economic losses."**

1

What if...

the United States were suddenly deprived of:

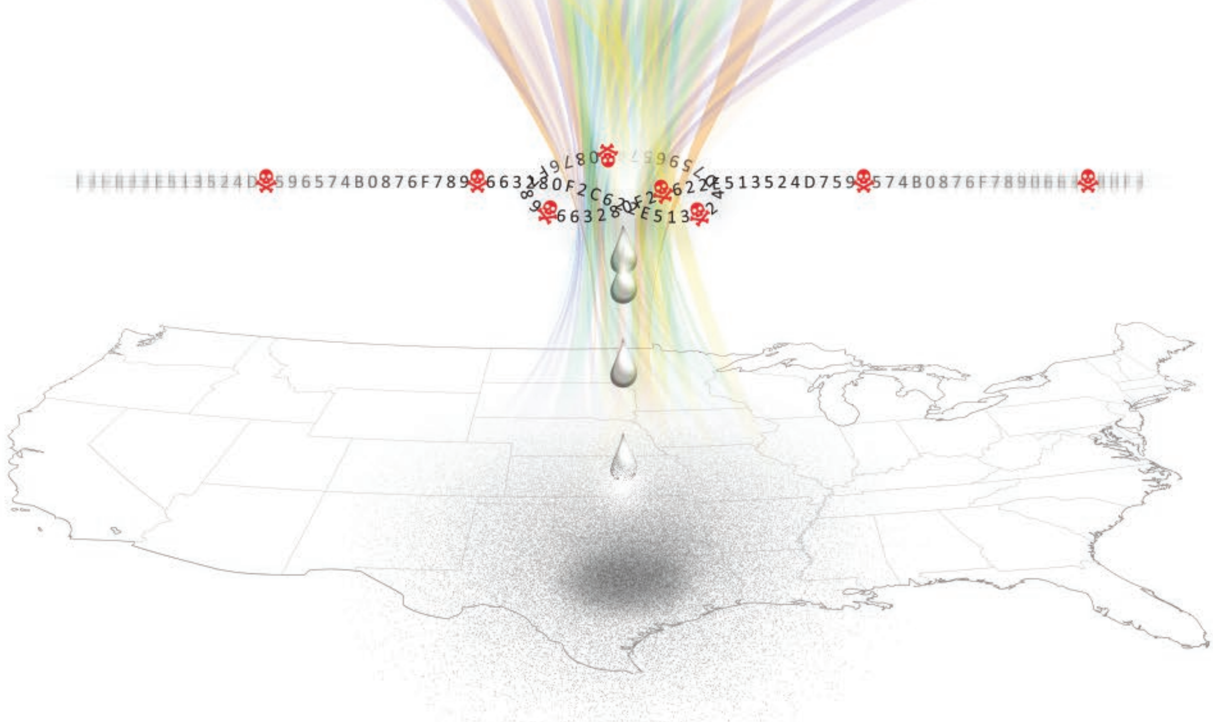
ELECTRICITY

WATER

MONEY

ACCESS TO CYBERSPACE

FUEL


E513524D 596574B0876F789 66328 0F2C62 0F2 622 E513524D759 574B0876F789
66328 E513 2

The infrastructure of the United States of America is a remarkable achievement of advanced science, technology, and commerce. Between transportation networks, commercial logistics, financial systems, power grids, telecommunications and more, Americans enjoy access, convenience, and reliability for nearly everything they need or want 24 hours a day.

This power and efficiency comes at a price: America's infrastructure is highly complex, interconnected, and deeply interdependent. Interdependence makes it vulnerable. The electric grid, for example, could be brought down without physically destroying a plant or a transformer. Attacks that disrupt any part of the power generation process or the systems that control them could bring down large sections of the electric grid and have a devastating impact on the rest of the country.

In addition to the threats facing physical infrastructure, America's way of life is not designed to withstand significant shocks. American commercial logistics systems, for example, are built for just-in-time inventory, and it is rare to have large stocks of goods ready and waiting at stores. It is only necessary to visit a supermarket before a severe storm to see that Americans are unprepared to subsist very long with an interruption to basic services. Threats that can interrupt these basic services, along with other pieces of critical infrastructure, fall into five categories: acts of terrorism, cyber threats, accidents or technical failures, extreme weather, and pandemics.[1] Over the last two decades, the United States has experienced numerous incidents that required national, regional, and local responses in all five categories.

ACCIDENTS OR TECHNICAL FAILURES
ACTS OF TERRORISM
PANDEMICS
CYBER THREATS
EXTREME WEATHER

▲ America's infrastructure continually faces significant threats to its basic services.

Exacerbating the vulnerability of America's critical infrastructure is the fact that no single organization has authority over it. Every element, from power generation and transmission, to water supplies, to the roads, railroads, and airports, is owned, operated, and maintained by a collection of private owners, public commissions, and public-private partnerships. It is estimated that 85 percent of the critical infrastructure in the United States is privately owned. In the absence of a single governing authority, vital elements of resilience and security must be negotiated among the owners and operators, rather than simply set by government.

The United States has developed significant institutional response capacity for most of these vulnerabilities and threats over the last decade, from counterterrorism plans and operations to

"... the United States and its people are simply unprepared to subsist very long with an interruption to basic services."

[1] U.S. Department of Homeland Security, Strategic National Risk Assessment, Dec. 2011 and NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Dec. 2013.

responses for natural and man-made disasters and pandemics. Prior to Hurricane Katrina, for example, the Federal Emergency Management Agency (FEMA) and United States Northern Command (NORTHCOM) seldom interacted, despite their closely connected responsibilities in the event of an emergency. Over the last decade, NORTHCOM has become "snap-linked" into FEMA and is ready to provide support as needed. Moving from reactive to proactive models of disaster response, Hurricanes Katrina and Sandy pushed FEMA and NORTHCOM to put together scenario-specific plans for joint responses to natural disasters. In addition to assessment teams that evaluate damage, the United States can now push capabilities and relief based on those plans and scenarios.

No such unified response capacity exists for threats to cyber systems throughout the United States' critical infrastructure. Consider the havoc a cyber attack can wreak. Cellular and land phone telephone lines and services become overloaded or unavailable. Television and radio stations go off the air. Water supplies are in danger of contamination, lacking the sensors and monitors used to regulate quality. Interstate, freight, and commuter rail services shut down. Service stations are unable to pump fuel, adding to massive traffic and transportation problems. Scores of factories are forced to shut down. ATMs cease to function. Hospitals lose significant capacity or shut down altogether.

Although this cascading chaos sounds like a Hollywood script, all of it actually happened when power went out during the August 2003 blackout, bringing life to a standstill for 55 million people in eight northeastern states and parts of Canada. The cause was strain to power lines during a heatwave and a previously unknown flaw in an alarm system's software. It triggered a domino effect

▲ **New Orleans, Louisiana in the aftermath of Hurricane Katrina.**

Photo by AP Photo/U.S. Coast Guard, Petty Officer 2nd Class Kyle Niemi

▲ **Manhattan suffered a widespread power outage caused by Hurricane Sandy.**

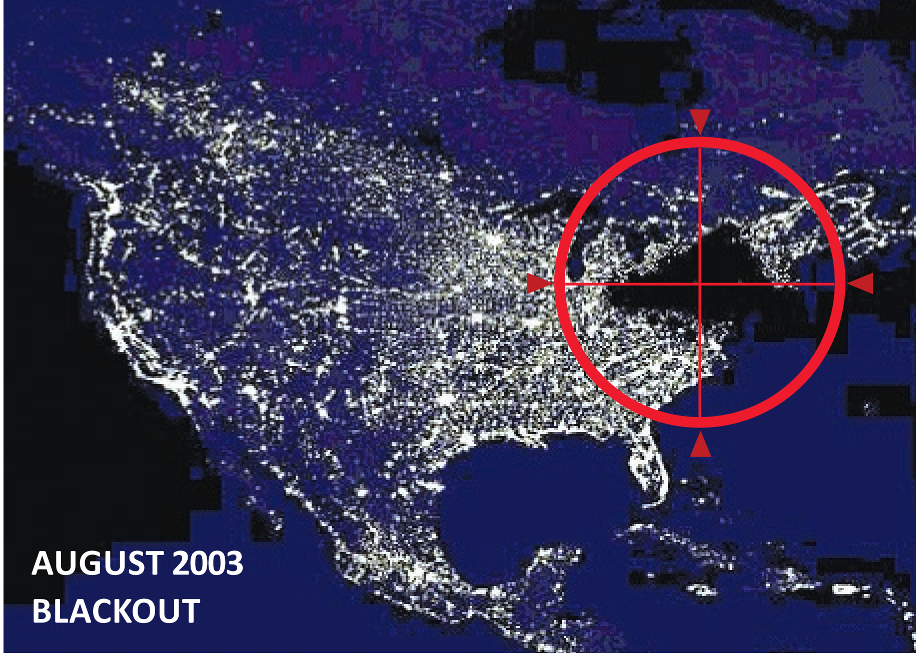
Photo by Hybirdd

“No unified response capacity exists for threats to cyber systems throughout the United States’ critical infrastructure. But cyber systems undergird America’s way of life.”

that rippled through some 100 other power plants to cause the shutdown and blackout situation. Estimated economic losses for the blackout were between $7 billion and $10 billion.

In 2003, the disruption to U.S. infrastructure was deemed accidental, but the power to do deliberate physical and economic harm through cyber attacks has grown rapidly since then. The Stuxnet virus, unleashed on Iran’s nuclear program, made the uranium-enriching centrifuges spin out of control while showing all gauges to be operating within normal parameters, physically damaging the centrifuges. Until then, physical damage could only be achieved through kinetic means like blast and fragmentation.

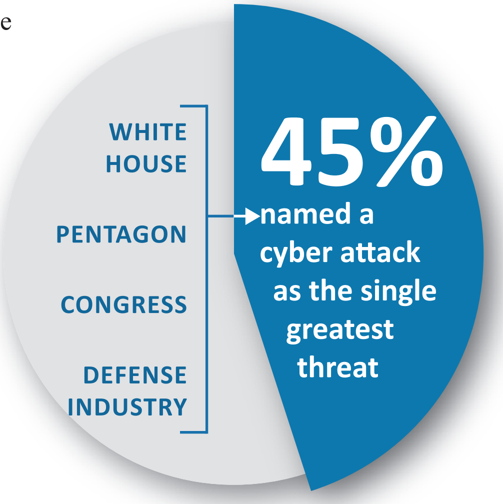
Americans have acknowledged the severity of cyber attacks. A Pew Research Center opinion poll conducted in December 2013 noted that 70 percent of people surveyed considered cyber attacks from other countries a major threat to the U.S.[2] Likewise, a more recent Defense News Leadership Poll, surveying senior officials at the White House, the Pentagon, in Congress, and in the defense industry concluded that 45 percent of the respondents named a cyber attack as the single greatest threat – nearly 20 percentage points above terrorism, which ranked second.[3]



▲ The 2003 North American blackout brought life to a standstill for 55 million people and triggered a domino effect that rippled through some 100 other power plants.

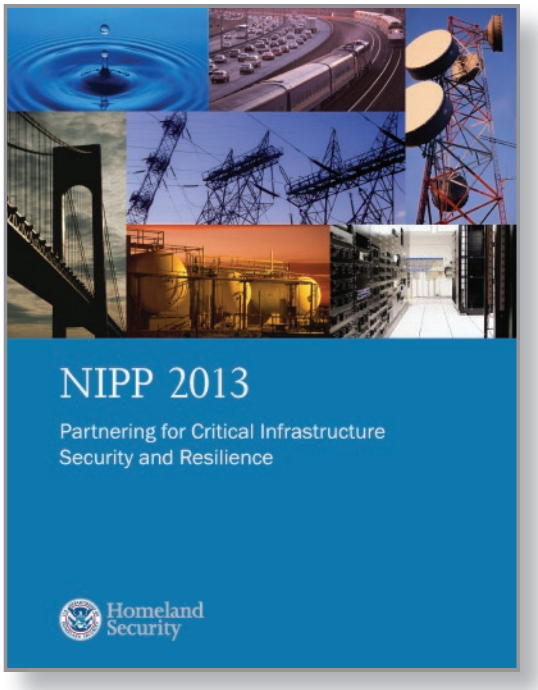
ISAT GeoStar 45 - 23:15 EST 14 Aug. 2003

The Department of Homeland Security (DHS) reports that more than 40 percent of the roughly 200 cases of hacking attacks handled by the Department’s cybersecurity team in 2013 were related to the energy sector. In 2013, several European and U.S. energy companies were also targets of industrial control system attacks that could have been used to disrupt energy supplies in those affected regions. In the private sector, hackers have breached computer networks at Sony,



[2] Pew Research Center, December 2013, “America’s Place in the World 2013.” http://www.people-press.org/files/legacy-pdf/12-3-13%20APW%20VI%20release.pdf. Accessed 2/5/2015.

[3] Zachary Fryer-Briggs, “Polls: Cyberwarfare Is Top Threat Facing US,” Defense News, Jan. 5, 2014 http://archive.defensenews.com/article/20140105/DEFREG02/301050011/Poll-Cyberwarfare-Top-Threat-Facing-US. Accessed 2/5/2015.


NIPP 2013
Partnering for Critical Infrastructure Security and Resilience
Homeland Security

The National Infrastructure Preparedness Plan is America's national plan to manage risks to U.S. infrastructure.

www.dhs.gov/national-infrastructure-protection-plan

Target, Lowe's Home Improvement, Citigroup, and the parent company of TJ Maxx, causing tens of millions of dollars in damage and loss of consumer confidence in cybersecurity.

To address the increasingly sophisticated threats that both the public and private sectors face, DHS developed an ongoing National Infrastructure Preparedness Plan (NIPP) "through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry." The NIPP is designed to "leverage partnerships, innovate for risk management, and focus on outcomes." In its 2013 iteration, the NIPP was promulgated as a national plan to streamline and adapt to existing risk, policy, and strategic environments and designed to facilitate "an integrated and collaborative approach to achieve the vision of a nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened." [4]

Such a comprehensive approach doesn't exist for cybersecurity. In 2014, the global cybersecurity market was said to be worth $77 billion.[5] However, the preponderance of money and effort is spent defending against the inherent vulnerabilities that exist in all complex systems. This defensive focus, especially perimeter defense that tries to keep attackers from gaining access in the first place, is simply not enough.

The U.S. urgently needs new approaches and authorities to ensure the resilience of its vulnerable critical infrastructure. The 16 critical infrastructure sectors have been integrated through DHS's array of Sector Coordinating Councils. These councils interact with a set of Government Coordinating Councils to develop standards for security and response. Likewise, the Department of Defense (DoD) and the Intelligence Community continue to develop innovative solutions to deliver C4ISR, EW, and other kinetic and non-kinetic effects in a contested, full-spectrum, electronic and cyber warfare environment. The ability to anticipate, plan for, coordinate, and execute operations against adversaries threatening the United States is paramount. The price of failure is nothing less than America's prosperity, global stature, and, ultimately, its very way of life.

"The U.S. urgently needs new approaches and authorities to ensure the resilience of its vulnerable critical infrastructure. "

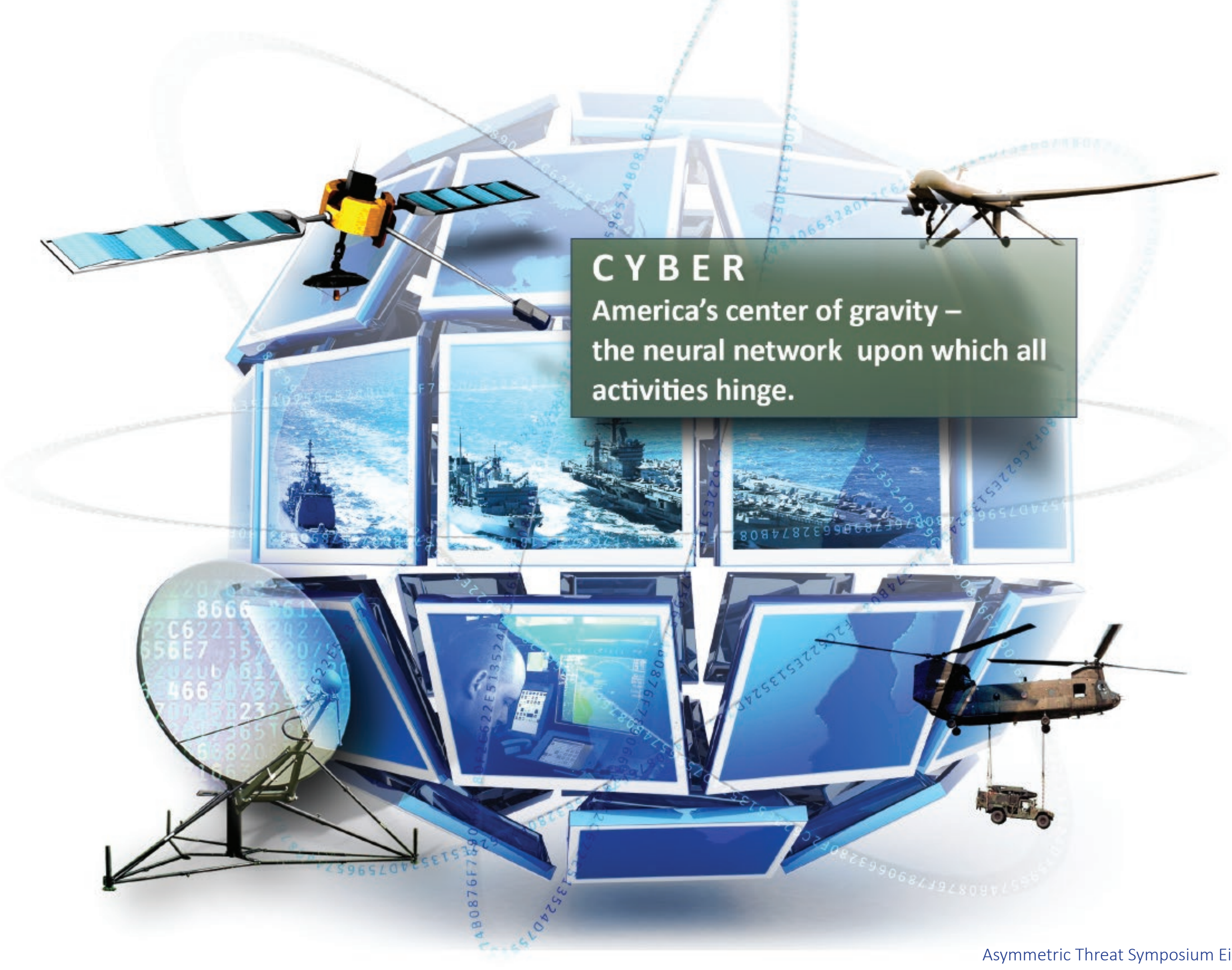
[4] U.S. Department of Homeland Security, NIPP 2013.

[5] Michael Peck, "Cyber Security Market to Hit $77B," The Federal Times, Feb 21, 2014 http://www.federaltimes.com/article/20140221/CYBER/302210004/Cybersecurity-market-hit-77B.

2 The Role of Cyber and Electronic Warfare in the Future Military Operational Environment

On March 4, 2014 – in the midst of the Crimean Crisis showcasing Russia's new assertiveness – President Barack Obama unveiled his 2015 Budget Request, seeking Congressional approval for $1.19 trillion in discretionary spending, plus another $56 billion for a new "Opportunity, Growth, and Security Initiative." The DoD portion of the request was $495 billion for the base budget – $6 billion less than in 2014. Factoring overseas contingency operations and both national and military intelligence programs – $45.6 billion and $13.3 billion, respectively – the downward spiral was unmistakable: $116 billion decrease in DoD topline, a 17 percent drop from the FY2010 peak in defense appropriations.

As required by law, the DoD Budget Request was accompanied by the Quadrennial Defense Review (QDR), which reflected "the transition DoD is making after 13 years of war … repositioning to focus on the strategic challenges and opportunities that will define [America's] future: new technologies, new centers of power, and a world that is growing more volatile, more unpredictable,



CYBER

America's center of gravity – the neural network upon which all activities hinge.

and … more threatening."[6] The next day, as if on cue, China announced a 12 percent increase in its own defense budget, which had already nearly doubled since the 2010 QDR, and Russia launched a "previously scheduled" ICBM test, alongside major land, sea, and air defense exercises. The shifting global balance – in perception, if not in reality – was unambiguous. Since then, Russia's actions against Ukraine have raised the specter of a new Cold War, refocusing U.S. attention on a theater that was thought to be peacefully settled for over two decades.

The 2014 QDR charts a strategy for an environment in which defense spending will steadily decline, while proliferation of advanced technologies means that American superiority can no longer be taken for granted. Cognizant of this reality, the QDR opts for an admittedly high-risk strategy: cutting force structure while "maintaining the technological edge." This approach reflects three difficult choices:

- Terminating or delaying some modernization programs to protect higher priority procurement;
- Slowing the growth of compensation costs to free up funds for training, reset, and readiness; and
- Further reducing force structure in every service – active and reserve – to sustain readiness and technological superiority, and to protect critical capabilities like special operations forces and cyber.

Concern with cyber is not new. It is, however, becoming increasingly visible. Military leaders – from the Chairman of the Joint Chiefs of Staff through service chiefs to combatant commanders – have repeatedly called attention to cyber and the EMS as top-priority requirements. The budget request accompanying the QDR included a $5 billion increase for unspecified "cyber programs."

"Cyber superiority is the prerequisite for effective operations in all domains – from the tactical to the central strategic levels."

Cyber is an operational domain defined by the physics of the EMS, electronics, and the infrastructures used to access and exploit their characteristics. As a domain, cyber is on par with land, sea, air, and space – vitally important to America's economic, political, diplomatic, financial, informational, and military power. Arguably, cyber is America's center of gravity – the neural network upon which all activities hinge. No nation is as reliant on and, consequently, as vulnerable in this domain as the United States. Cyber superiority is the prerequisite for effective operations in all domains – from the tactical to the central strategic levels. Cyber enables such everyday functions as power generation, transport and traffic control, industrial processes, global positioning, navigation and timing, communications, intelligence collection in all disciplines, logistics, security, and financial and legal transactions, among others.

Militarily, cyber comprises all operations conducted in and through the EMS, from C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance), through computer network defense, exploitation and attack, to electronic warfare (EW), directed energy weapons, electromagnetic pulse, and technologies not yet conceived. By its very nature, cyber favors the offense. Good security practices are vital, but focusing entirely on defense is akin to the medieval practice of building thicker castle walls or digging deeper moats. The United States must field knowledge-centric systems that process, filter, integrate, and convey data in ways that enable quick, logical decisions. Self-forming, self-healing networks are required to fight through and prevail in EMS-denied environments.

[6] Department of Defense, Quadrennial Defense Review Report, Mar. 2014. Accessed Feb. 2015.

Though the cyber domain is highly sophisticated, the cost of entry is comparatively low. Electronic attacks are widely seen as a relatively cheap and easy way to wreak havoc on an unprecedented scale. Dual-use, readily-available technologies abound: a cell phone is a ubiquitous communications device, or an improvised explosive device (IED) detonator; an iPad offers video and email on demand; it can also overpressure a gas main or make traffic signals go haywire. Trillions of dollars in global electronic transactions offer a lucrative target. Not surprisingly, cyberspace is rife with criminals, terrorists, and nation states seeking a high-impact, low-cost asymmetric advantage.

The race is to the swift: whoever masters the EMS and denies it to the adversary, wins. To this end, Chinese information operations and cyber units have been fully integrated with EW to operate across the EMS. Likewise, specialized Russian units target computer networks and train for high-end terrestrial and space-based "radio-electronic combat." Both Russia and China, as well as other state and non-state actors, field advanced encryption-cracking capabilities to penetrate, corrupt, or co-opt opposing systems. The electron is fast becoming the ultimate precision-guided munition – capable of devastating the target's economy, infrastructure, and military.

The first battle of any future war will be for command and dominance of space and the EMS. Yet the U.S. is neither adequately prepared to counter the growing threat, nor armed with sufficiently robust capabilities. As America's strategic focus shifts away from conflicts in which it held an overwhelming technological advantage to operations in anti-access and area denial environments, against adversaries who command both economic heft and sophisticated technologies, superiority can no longer be taken for granted. The United States urgently needs new methods to deliver C4ISR, EW, and other kinetic and non-kinetic effects in a contested, full-spectrum EW/cyber warfare environment. The ability to anticipate, plan for, and execute operations against enhanced adversary capabilities – exploiting opponents' vulnerabilities while compensating for America's own – will be paramount.

◀ **Cyberspace is rife with criminals, terrorists, and nation states seeking a high-impact, low-cost asymmetric advantage.**

The United States needs the skills, tools, and expertise to deliver the defensive and offensive solutions required to prevail in increasingly contested and dangerous environments. As the demand for global C4ISR grows, so does reliance on assured access to space and the EMS. The challenge is to find affordable pathways to secure both, balancing hardening, countermeasures, and reconstitution.

The most recent historical parallels to operations in cyber and the EMS are mastery of the air and space domains. Both were quickly assessed as strategically vital, but superiority required an extraordinary commitment of will, intellect, and resources. It is worth recalling that it was the Soviet Union that launched Sputnik – the world's first artificial satellite – kicking off a space race which it ultimately lost, exhausting its economy to the brink of collapse in the process.

America's global military posture hinges on technological superiority in all domains. As EMS and cyber technologies become more ubiquitous and readily accessible, America's advantage dwindles, particularly since most offsetting capabilities rely heavily on a technological edge in electronics, software, and network connectivity.

"In an era when the speed of information exceeds the speed of engagement, the synchronization of cyber and EW capabilities is critical."

In an era when the speed of information exceeds the speed of engagement, the synchronization of cyber and EW capabilities is critical. The continuing growth of networked systems, devices, and platforms means that EMS operations are embedded into an increasing number of capabilities that DoD relies upon to accomplish its missions. Cyber and EW enable the hundreds of billions of dollars invested in weapons systems upon which the Joint Force depends. Their networked connectivity is a dominating strength; their fragility is an exploitable weakness. If the United States is to maintain its strategic advantage, enhanced control of its networks and a higher confidence in the security and integrity of the data transmitted over these networks are vital to success.

Unimpeded access to the EMS is a prerequisite for modern military operations. DoD's ever-increasing requirements to gather, analyze, and share information rapidly; to control a growing number of automated C4ISR assets; to command geographically dispersed and mobile forces; and to gain and maintain access to denied areas all require realistic training and assured spectrum access.

The offensive and defensive effects that the warfighter requires are achieved through credible military actions orchestrated in time, space, and purpose in order to produce maximum combat power at a decisive place and time. The four service branches have taken key steps to integrate cyber and EW. Several years ago, the U.S. Navy reorganized its cyber forces into an operational command, Fleet Cyber Command/U.S. 10th Fleet. This structure enables the Navy to organize, command, and control its cyber and electromagnetic forces from a single operational command. Likewise, the U.S. Air Force stood up the 24th Air Force, and the Army organized a cyber command known as ARCYBER. At the Joint level, the U.S. Cyber Command was stood up as a sub-unified command under the U.S. Strategic Command.

Under Title X of U.S. Code, it is the mission of the military services to "organize, train, and equip" combat-ready forces and present those forces to the unified commanders for employment in accordance with Joint Operational Plans and Concept Plans, as well as Joint Task Forces constituted to respond to emerging, often unanticipated requirements. The services don't employ forces; the Joint Commanders do. Accordingly, each service has been working diligently to recruit, train, and retain the requisite cadre of "cyber warriors" to support both the regional and functional

◀ **USCYBERCOM centralizes command of cyberspace.**

combatant commands, including USCYBERCOM collocated with the National Security Agency at Ft. Meade, MD.

Joint doctrine is designed to provide the “sheet music” to guide the services as they discharge their Title X responsibilities. To this end, Joint Publication (JP) 3-12 Cyberspace Operations was released on February 5, 2013. It defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

JP 3-12 separates cyberspace operations into two categories: offensive and defensive. Offensive operations project power by the application of force in and through cyberspace. Defensive operations are active and passive operations to preserve the ability to use friendly cyberspace capabilities.

As dependence on the network continues to grow, combatant commanders are well aware that the EMS is as vital as the weapons it powers.

▲ **A MQ-9 Reaper unmanned aerial vehicle used in Afghanistan and in other operations, including current operations against ISIS.**

Between Operation Desert Storm and Operation Iraqi Freedom (OIF), information needs and communications availability rose exponentially to support a markedly smaller force structure, more heavily reliant on unmanned aerial vehicles and C4ISR systems that required significant bandwidth and unimpeded access to the EMS.[7] Between Operation Enduring Freedom in Afghanistan in 2001 and OIF, there was further growth in the demand for bandwidth. More than 50 times more bandwidth was used per person in OIF than in Desert Storm.[8] The requirements for additional unmanned systems and C4ISR continue unabated.

The synchronization of cyber and EW is key to victory in future conflicts. Those conflicts will not be won simply by using the EMS and cyber; rather, they will be won within the EMS and cyberspace. This, in turn, will lead to changes in operating concepts, systems, and – most importantly – thinking about conflict itself. Future conflicts will be coordinated, synchronized, and fought in the land, sea, air, space, and cyber domains using the EMS with both legacy and emerging platforms. To prevail in this future operational environment, DoD needs a structured governance organization that focuses on Joint and defense-wide EMS capabilities; emphasizes the need to doctrinally and physically synchronize and employ cyber and EW; and rationalizes additional investment requirements.

The Joint Staff, the Undersecretary of Defense for Policy, U.S. Cyber Command, and the United States Strategic Command (USSTRATCOM) are addressing synchronization of force application across the spectrum and have developed a draft construct to provide this overarching guidance. Under a relatively new concept of operations, the Commander of USSTRATCOM is responsible for joint EW, including advocating for joint EW capabilities, providing contingency EW support

[7] Jay H. Anson, “Leaders are the Network: Applying the Kotter Model in Shaping Future Information Systems,” Page 11, figure 2 “USAF C4 Infrastructure OIF vs. ODS.”

[8] Harry D. Raduege, “Net-Centric Warfare is Changing the Battlefield Environment,” Crosstalk: The Journal of Defense Software Engineering 17, no. 1 (January 2004): 7-8.

to other commands, and supporting combatant commands joint training and planning related to controlling the EMS. These organizations are working to better define and clarify the existing shared space between the electronic and cyber attack mission areas in order to properly validate requirements and develop enhanced capabilities. This is another critical initial step in closing the EMS gap for America's warfighters.[9]

"The electron is fast becoming the ultimate precision-guided munition."

The entire acquisition system – from the identification of new threats to the fielding of new capabilities – is too slow for a world in which Moore's Law doubles computing power every 18 months and software-defined systems can change their entire electromagnetic profile mid-mission. The scale of the cyber and EW problems makes the remedies expensive in an era of declining defense budgets and competing missions.

The explosion of computing power, mobile devices, and widely available access to the EMS means that the United States can no longer assume it has command of the domain. Rapid commercial and consumer adoption means that technologies once available only to nation states and multinational corporations are now found on the shelves of Best Buy and Target. Disruptive military technology could come from a few modems and a computer terminal.

Four elements underpin national military power: speed, stealth, precision, and persistence. These four elements have been core to military dominance since time immemorial. However, the character of these elements has fundamentally changed. Speed is no longer just ground speed, air speed, or nautical speed; it is the speed of decision-making – the speed of light. Stealth is not merely an unexpected approach or low-observable platform; it requires delivering effects undetected. And as conflict moves from a permissive to a contested environment, precision is becoming all the more critical. The electron is the new precision-guided munition. Persistence is no longer defined by a campaign season, limited in scope and duration. It means an unblinking eye and an ever-functioning brain, 24 hours a day, every day. Cyber is the neural network undergirding all modern operations, in all domains. Like oxygen, the EMS is simply indispensable.

"The explosion of computing power, mobile devices, and widely available access to the EMS means that the United States can no longer assume it has command of the domain."

[9] Joint Electromagnetic Spectrum Operations (JMSO), USSTRATCOM December 2011, www.stratcom.mil/factsheets/16/JEMSO/.

3 The Electric Grid, the All-Hazards Approach, and the National Infrastructure Preparedness Plan

Cyberspace and the EMS are vital to America's national security and to its economic, diplomatic, and military pre-eminence in the world. Those vital components, however, are themselves dependent on a third critical infrastructure: the nation's bulk power distribution system, better known as the electric grid. Because of its unique significance, the electric grid provides an object lesson for the all-hazards approach to critical infrastructure protection and the NIPP.

Critical infrastructure is like a house of cards: remove one card, and the entire structure weakens or collapses. For the United States, that one card is the electric grid. All other critical infrastructures are dependent upon reliable supplies of power. The grid itself is vulnerable to all of the same threats as other critical infrastructures, like cyber warfare and physical sabotage. But it also faces unique threats. The nation's electrical grid relies on nearly 45,000 substations and approximately 350 high-voltage transformers, which are manufactured almost exclusively overseas and can take over a year

◂ **Critical infrastructure is like a house of cards: remove one card, and the entire structure collapses. For the United States, that one card is the electric grid.**

to produce. Destroying or disabling any one of them could result in catastrophic power failures. Furthermore, the electric grid, as well as electronic devices, are subject to the unique threat of electromagnetic pulse (EMP).

Every industrialized nation, and particularly the United States, faces a dangerous vulnerability of its electronic systems to intentional interference by the high-altitude detonation of a nuclear weapon or by localized attacks using radio frequency weapons. There are also naturally occurring EMPs caused by intense solar storms that are vectored directly at the Earth roughly every 150 years. (The last such storm, known as the Carrington Event, occurred in 1859. Telegraph systems and infrastructure worldwide were damaged, shocking telegraph operators and setting telegraph paper on fire.) Since then, electronics have become significantly more effective and more widespread and, therefore, more vulnerable to the ravages of an EMP. Should the grid go down for any length of time, it poses a significant threat to the nation.

▲ Naturally occurring EMPs can be caused by intense solar storms.

By NASA Goddard Space Flight Center

The vulnerability of the U.S. electric grid is well known to America's potential adversaries. Many of those adversaries have the capacity to engage in what could be devastating attacks aimed at disrupting, if not destroying outright, key grid assets like high-voltage transformers and network control systems for protracted periods. This situation – a nuclear attack on the U.S. electric grid by a potential adversary like Iran or North Korea – is a major danger to the United States. Against this backdrop, questions arise as to the adequacy of federal, state, and local government efforts to assure the resiliency of the U.S. electrical grid and associated critical infrastructure: How can policy makers measure the adequacy of these preparatory efforts? Given that roughly 85 percent of the bulk power distribution system is owned and operated by the private sector, what sorts of public-private partnerships are needed to meet both existing and future threats? And are these efforts being adequately considered, resourced, coordinated, and exercised?

The National Infrastructure Protection Plan (NIPP) was created to organize the protection of critical infrastructure assets from naturally occurring risks and targeted threats by various adversaries. Over time, it evolved to incorporate the protection and resilience of cyber capabilities and infrastructure as well as management of aspects of the EMS. Initially, it was unclear how to incorporate the strategic risks of EMP, geomagnetic disturbances, solar storms, or catastrophic threats into the NIPP. It seems to have been unclear how to implement the kinds of critical infrastructure protections in the private sector electrical industry that are done for government-owned assets – even though, ironically, the majority of DoD facilities in the United States rely on the civilian power grid.

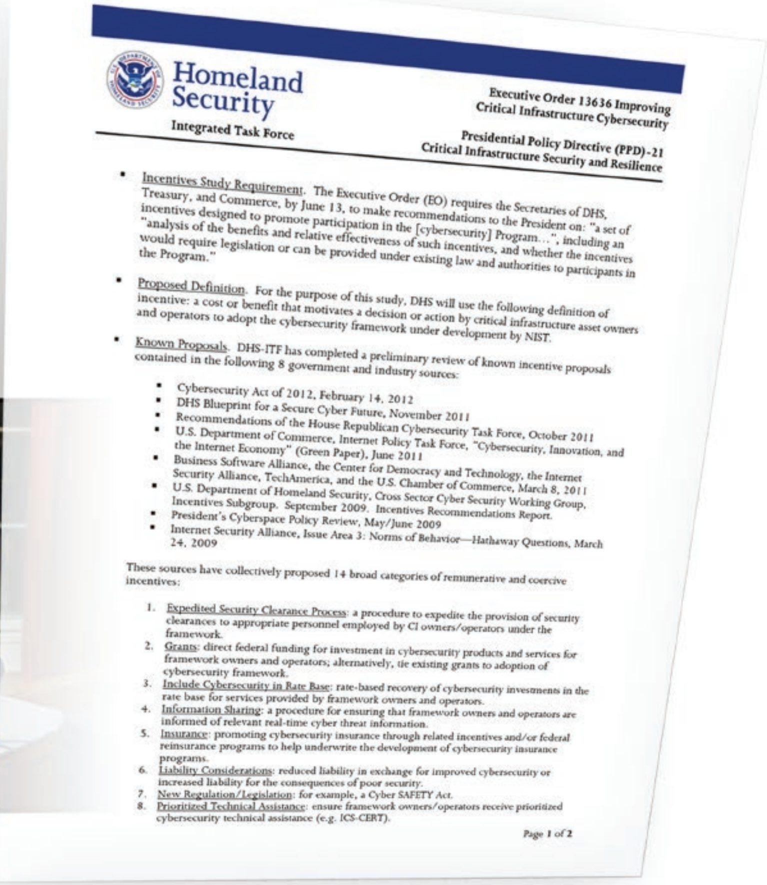
President George W. Bush.
White House photo by Eric Draper

Following the creation of DHS, President George W. Bush issued “Homeland Security Presidential Directive 7” (HSPD-7), which set out the national policy for the federal government to identify, prioritize, and protect critical infrastructure. It also defined the responsibilities for DHS and selected federal agencies – known as sector-specific agencies (SSAs) – that lead collaboration within an industry sector to create a sector-wide plan that applies the principles of the NIPP. The NIPP identifies 16 sectors of critical infrastructure, including manufacturing, chemicals, communications, energy, and financial services, each with an SSA.

On February 12, 2013, President Obama took the protection of critical infrastructure further, explicitly integrating cybersecurity. He signed Executive Order 13636, “Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience,” which required DHS, in coordination with the SSAs, to “use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” This was a necessary step to apply the highest standard of risk assessment to both cyber infrastructure and the interrelations of all sectors.

Despite the challenges of securing infrastructure of such a massive scale and scope, the NIPP is still a comprehensive and progressive approach. One key tenet of the NIPP is risk management across all hazards. This entails understanding what infrastructure is critical, particularly a focus on critical life functions, but also recognizing that risk management includes businesses and governments making tradeoff decisions on a regular basis. The challenge is magnified by the complexity of critical infrastructure’s interdependence, across sectors and across borders.

▼ President Barack Obama signs Executive Order 13636.
White House photo by Eric Draper



Homeland Security
Integrated Task Force

Executive Order 13636 Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience

- Incentives Study Requirement. The Executive Order (EO) requires the Secretaries of DHS, Treasury, and Commerce, by June 13, to make recommendations to the President on: "a set of incentives designed to promote participation in the [cybersecurity] Program…", including an "analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program."
- Proposed Definition. For the purpose of this study, DHS will use the following definition of incentive: a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the cybersecurity framework under development by NIST.
- Known Proposals. DHS-ITF has completed a preliminary review of known incentive proposals contained in the following 8 government and industry sources:
    - Cybersecurity Act of 2012, February 14, 2012
    - DHS Blueprint for a Secure Cyber Future, November 2011
    - Recommendations of the House Republican Cybersecurity Task Force, October 2011
    - U.S. Department of Commerce, Internet Policy Task Force, "Cybersecurity, Innovation, and the Internet Economy" (Green Paper), June 2011
    - Business Software Alliance, the Center for Democracy and Technology, the Internet Security Alliance, TechAmerica, and the U.S. Chamber of Commerce, March 8, 2011
    - U.S. Department of Homeland Security, Cross Sector Cyber Security Working Group, Incentives Subgroup. September 2009. Incentives Recommendations Report.
    - President's Cyberspace Policy Review, May/June 2009
    - Internet Security Alliance, Issue Area 3: Norms of Behavior—Hathaway Questions, March 24, 2009

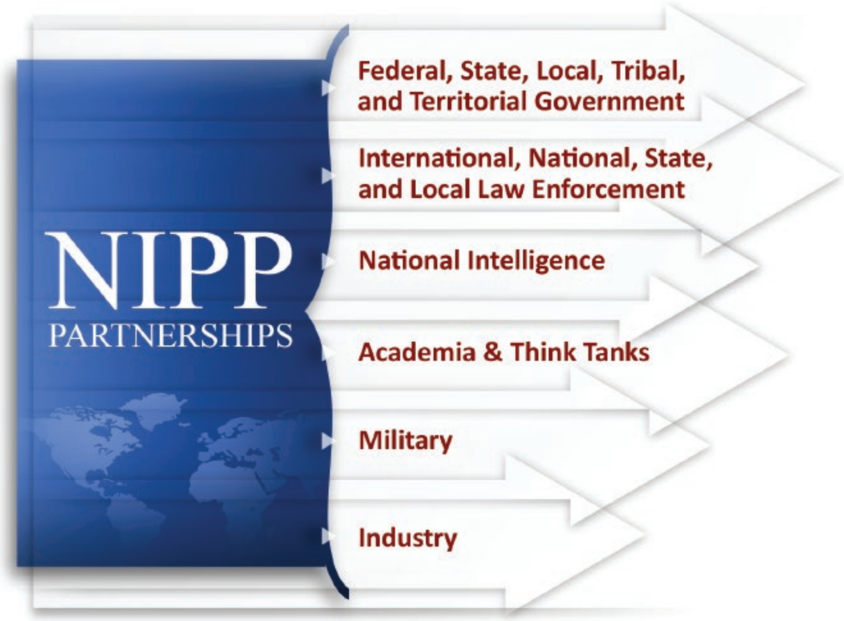
These sources have collectively proposed 14 broad categories of remunerative and coercive incentives:

1. Expedited Security Clearance Process: a procedure to expedite the provision of security clearances to appropriate personnel employed by CI owners/operators under the framework.
2. Grants: direct federal funding for investment in cybersecurity products and services for framework owners and operators; alternatively, tie existing grants to adoption of cybersecurity framework.
3. Include Cybersecurity in Rate Base: rate-based recovery of cybersecurity investments in the rate base for services provided by framework owners and operators.
4. Information Sharing: a procedure for ensuring that framework owners and operators are informed of relevant real-time cyber threat information.
5. Insurance: promoting cybersecurity insurance through related incentives and/or federal reinsurance programs to help underwrite the development of cybersecurity insurance programs.
6. Liability Considerations: reduced liability in exchange for improved cybersecurity or increased liability for the consequences of poor security.
7. New Regulation/Legislation: for example, a Cyber SAFETY Act.
8. Prioritized Technical Assistance: ensure framework owners/operators receive prioritized cybersecurity technical assistance (e.g. ICS-CERT).

Page 1 of 2

To help all parties arrive at the best decisions, the second key tenet of the NIPP is promoting better multidirectional, information-sharing across the government, industry, and public. In being given responsibility for the NIPP, DHS was empowered to lead, coordinate, and foster a framework of public and private partnerships to tackle the infrastructure protection issue.

Fostering these public-private partnerships is the third key tenet of the NIPP. Government organizations bring key authorities and capabilities to the NIPP, but they have to rely on the expertise of the private sector for much of the command, control, and execution. Experience has shown that competing interests and the lack of authoritative regulatory ability can impede improvements to the security and resilience of critical infrastructure. DHS has had to develop a planning process that had the private sector at the table from the outset, that involved all levels of government, and that brought together parts of the federal government that have not always collaborated effectively.


NIPP
PARTNERSHIPS
Federal, State, Local, Tribal, and Territorial Government
International, National, State, and Local Law Enforcement
National Intelligence
Academia & Think Tanks
Military
Industry

> “The overriding challenge facing efforts to address the security of critical infrastructure is that, ultimately, no single organization has responsibility for infrastructure.”

A possible model for partnerships may be found by looking at Pentagon and industry cooperation on cyber threats. DoD is rarely accused of moving quickly to solve a problem. But in the case of cyber espionage, cyber warfare, and other threats, the relationship that the Pentagon has with its contractors enabled it to get ahead of the curve in some respects. DoD began developing and utilizing a public-private partnership approach circa 2007 in response to a particular cyber-compromise of a major defense contractor. It took considerable time to devise and implement this still-evolving partnership.

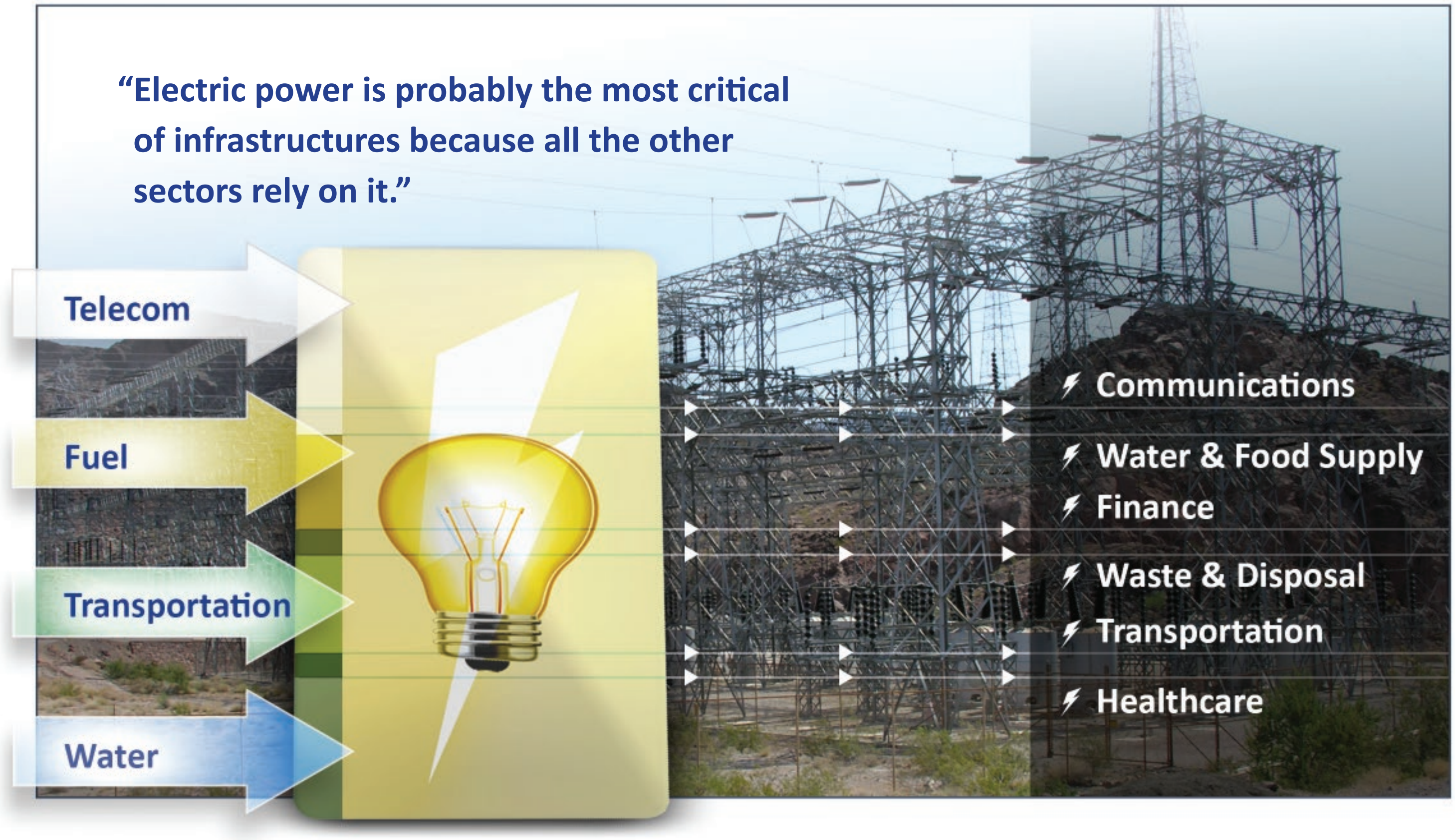
The final key tenet of the NIPP is a call for collective action. DHS and the NIPP were never envisioned or authorized to be the sole owners and managers of such a complex challenge. The NIPP’s purpose is to plan for networked governance and partnership because surmounting these challenges requires unleashing combined national capabilities. Such collective action and capabilities include: improved understanding of the systems that are in play; knowing what is critical; building near real-time situational awareness; and recognizing cascading impacts and interdependencies. The NIPP’s success is dependent on government at all levels, national and international law enforcement, the Intelligence Community, and the military, as well as non-governmental organizations, think tanks, academia, and industry.

A possible model for partnerships in protecting the electric grid and other critical infrastructures from asymmetric attacks can be found by looking at Pentagon and industry cooperation on cyber threats.

As a result, there is a great need for these DHS-led NIPP missions to reach and sustain a level of readiness and action similar to that expected of the Armed Forces. This is the level of readiness and preparedness needed to overmatch a particular threat and have the agility and resilience to prevail against the threat over time. And this readiness – for now – must be achieved in the absence of a singular governing authority or body.

Measuring the readiness and preparedness of the NIPP against these tenets is also a Herculean task. It is necessary to measure each sector, the interdependencies among the sectors, and the probability that the NIPP will work against a hybrid event such as a cyber attack against the healthcare system during a pandemic. One also has to measure the level of training and preparedness of the people and institutions that need to implement the plan and respond to the subsequent resiliency challenges. In the private healthcare sector, for example, there are 13,000,000 healthcare professionals; 3,905 hospitals; 545,000 ambulatory healthcare services; 75,000 nursing homes; 42,000 pharmacies; and 1,100 pharmaceutical manufacturers.[10] Training, standardization, and information-sharing within this sector is a daunting task and difficult to adequately measure from a readiness standpoint. Add to this the healthcare and public health sector dependency on support from other sectors like energy for electricity and fuel to power facilities and vehicles. Furthermore, healthcare is just as dependent on information technology and communications as every other sector.

[10] 2010 Healthcare and Public Health Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, U.S. Department of Homeland Security and Department of Health and Human Services. Table 1-1: Healthcare and Public Healthcare and Public Health Sector Statistics, p 11.



“Electric power is probably the most critical of infrastructures because all the other sectors rely on it.”

Meanwhile, the other sectors are dependent on healthcare to provide services to their workforces to sustain operations. The healthcare sector is just one example of the magnitude of the challenges facing the NIPP and national security.

Despite the challenges, it is crucial to have protections in place that are commensurate with the risk and the magnitude of the loss across every sector. In the case of critical infrastructure protection, there is some dispute over whether risk management and mitigation are the correct approaches when dealing with existential threats, such as those posed by the loss of the electric grid.

It is impossible to be secure from all threats at all times. For most threats, the risk management approach is likely the appropriate one.

Resilience – the ability to recover quickly in the event of an accident, attack, or disaster, and the elimination of single points of failure – ought to be the objective. The electric utilities industry, for example, seeks to address the resiliency challenge by developing and adopting standards for protecting against various hazards they generate; using technology to improve situational awareness, share critical information in a timely way, and perform efficient incident response.

“Resilience – the ability to recover quickly in the event of an accident, attack, or disaster, and the elimination of single points of failure – ought to be the objective.”

That said, industry per se does not have intelligence-gathering capabilities, or law enforcement responsibility, or, as a general matter, national security expertise. These are functions that belong, properly, to the government of a nation state and not the private sector. This means that, even though government does not own critical infrastructure like the electric grid, it has a very real role to play. It is only prudent that government should be closely linked with industry in planning, setting standards, and protecting the grid, as well as all critical infrastructure.

There is one threat that may require 100 percent security, however: the threat posed by EMPs to electronics and the electric grid. As discussed earlier, an EMP, whether man-made or natural, could pose an existential threat to America's way of life. The grid is a relatively soft target, dispersed over a continent with tens of thousands of access points to defend. An attacker, or a solar flare, only needs to hit one station with sufficient force in order to bring swathes of American life to a grinding, agonizing halt.

The EMP Threat Commission Chairman, Dr. William Graham, estimates that nine out of ten Americans will not survive if the power goes out and stays out over a protracted period of time. That prospect should concentrate the minds of America's top strategic thinkers to resolve the all-hazards asymmetric threat to the electric grid, and the rest of America's critical infrastructure, as quickly as possible.

"The grid is a relatively soft target, dispersed over a continent with tens of thousands of access points to defend. An attacker, or a solar flare, only needs to hit one station with sufficient force in order to bring swathes of American life to a grinding, agonizing halt."

4 Conclusions and Recommendations

America faces real threats to its critical infrastructure, to its position in the world, and to its way of life from peer states, rogue states, non-state actors, and natural phenomena. The magnitude of the threat derives from the interconnection and interdependence of America's critical infrastructure, the vulnerability of the electric grid, and America's reliance on cyberspace. Further, America's national security is inextricably linked to dominance in cyberspace and the electromagnetic spectrum. The country has taken key steps to address these weaknesses, such as establishing the National Infrastructure Protection Plan (NIPP), creating public-private partnerships for security, and standing up cyber commands in DoD. There is still work to do, however, to address America's resilience against the threats it faces.

Recommendation 1 – Gain and maintain dominance over and freedom of access across the electromagnetic spectrum (EMS) – a major underpinning of national security planning.

From this point forward, the U.S. should expect to be challenged at home and abroad in all domains, including in and through space and cyberspace, across the EMS, as well as on land, at sea, and in the air. The U.S. must not only secure such freedom of access but also gain and maintain dominance of the EMS to ensure national security. It will be equally important for the United States to be able to deny its adversaries access to the EMS. With this in mind, U.S. access to and, indeed, dominance of the spectrum should underpin national security planning and resource commitments. The race is to the swift: he who masters the EMS and denies it to an adversary, wins.

Recommendation 2 – Further integrate electronic warfare and cyber operations in both military doctrine and planning as well as in research and development for national security capabilities.

The ability to plan and execute operations against adversaries capable of simultaneously threatening American civilians and harming U.S. Armed Forces is paramount. The country should continue to integrate cyber operations and electronic warfare, not only into military operations and planning, but also into research and development. The DoD and the Intelligence Community require immediate, innovative solutions to deliver C4ISR, cyber, electronic warfare, and related kinetic and non-kinetic effects in a contested, full-spectrum, electronic, and cyber warfare environment.

Recommendation 3 – Strengthen support, resourcing, and authorities for the NIPP.

Strengthening the security and resilience of the electric grid and cyber infrastructure that undergird so much of America's way of life is essential. The interdependencies – and vulnerabilities – of American infrastructure are well-known to adversaries. Continuing the NIPP's evolution, provide more rigorous and comprehensive cross-industry training and periodic exercising of the NIPP to assure protection and resilience goals are met.

Recommendation 4 – Foster public-private partnerships that provide trusted collaboration to prevent, secure, and mitigate the impact of electromagnetic spectrum hazards, cyber attacks, and insider threats.

It will be necessary to continue building strong partnerships at all levels of government, both nationally and internationally, and between government and industry. The U.S. should continue to foster public-private partnerships that provide trusted collaborative practices and training to secure, protect, and mitigate the effects of cyber attacks, insider threats, and EMS hazards such as EMPs.

Recommendation 5 – Enact comprehensive cyber legislation to confer authorities, assign responsibilities, define reporting relationships, and resolve privacy and liability issues to facilitate the degree and speed of information-sharing required for electromagnetic spectrum management and cyberspace.

The country requires comprehensive legislation and policy governing cyberspace and the EMS. Comprehensive cyber legislation and policy would also include strengthening rapidly evolving international laws and conventions, as well as the non-governmental and private sector partnerships that promote cybersecurity and freedom of access to cyberspace.

To triumph against today's and tomorrow's threat array, the U.S. must retain the freedom to attack, and the freedom from attack, in and through terrain, atmosphere, oceans, space, and the EMS. This, in turn, requires integrating systems, capabilities, organizations, branches of government, and operations to maximize the synergies that generate simultaneous, synchronized effects on land, at sea, in the air, space, and cyberspace – all while defending American interests, to include its critical infrastructure.

The threats facing the United States in cybersecurity, electronic warfare, and critical infrastructure are pervasive, but not insurmountable. In order to prevail against these threats, the United States must aggressively pursue a comprehensive national security policy that ensures the nation's resilience in the face of hazards to its critical infrastructure and use of the EMS.

> **"The race is to the swift:**
> **he who masters the EMS and**
> **denies it to an adversary, wins."**

5 Glossary

All hazards threat – A threat or an incident that warrants action to protect life, property, the environment, or public health and safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience)

Critical infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (USA Patriot Act of 2001)

Cybersecurity – The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. This includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (2009 National Infrastructure Protection Plan)

Cyberspace – A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-12 Cyberspace Operations)

Cyber superiority – The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-12 Cyberspace Operations)

Defensive cyberspace operations – Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Directed energy – An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-13.1 Electronic Warfare)

Electric grid – The interconnected network for delivering electricity from suppliers to consumers. It comprises generating stations that produce electrical power, high-voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers.

Electromagnetic pulse – The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. Also called EMP. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-13.1 Electronic Warfare)

Electromagnetic spectrum – The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-13.1 Electronic Warfare)

Electronic attack – Division of electronic warfare using electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-13.1 Electronic Warfare)

Electronic warfare – Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-13.1 Electronic Warfare)

Government Coordinating Councils (GCCs) – The government counterpart to the Sector Coordinating Council for each sector of critical infrastructure, established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government as appropriate to the risk and operational landscape of each sector. (2009 National Infrastructure Protection Plan)

National Infrastructure Protection Plan (NIPP) – NIPP 2013: Partnering for Critical Infrastructure Security and Resilience outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

Offensive cyberspace operations – Cyberspace operations intended to project power by the application of force in or through cyberspace.

Precision-guided munition – A guided weapon intended to destroy a point target and minimize collateral damage. Also called PGM, smart weapon, smart munition. (JP 1-02 Department of Defense Dictionary of Military Terms, JP 3-03 Joint Interdiction)

Radio-electronic combat – The total integration of EW and physical destruction resources to deny the use of electronic control systems. It also protects friendly electronic control systems from disruption by the enemy.

Sector Coordinating Councils (SCCs) – The private sector counterparts to GCCs, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector of critical infrastructure; serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (2009 National Infrastructure Protection Plan)

Sector Specific Agencies – A federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (2009 National Infrastructure Protection Plan)

Acknowledgements

Symposium Participants
(in alphabetical order)

Scott Aaronson
Senior Director National Security Policy, Edison Electric Institute

Ken Asbury
President and Chief Executive Officer, CACI International Inc

Mr. Asbury also served as Advisor

Daniel R. Ennis
Director, NSA/CSS Threat Operations Center (NTOC)

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

Richard M. Gray
Associate General Counsel, Department of Defense

COL William J. Hartman, USA
Commander, 780th Military Intelligence Brigade, U.S. Army Cyber Command

Maj Gen Kenneth R. Israel, USAF (Ret)
Acting President and President-Elect, Association of Old Crows

Maj Gen (Ret) Israel also served as Advisor

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

Dr. Kass also served as Advisor

Robert Kolasky
Senior Policy Advisor and Director of Strategy and Policy, Office of Infrastructure Protection, Department of Homeland Security

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

Maj Gen Jeff Newell, USAF
Director of Strategy, Policy and Plans (J5), North American Aerospace Defense Command and United States Northern Command

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

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate (NPPD), Department of Homeland Security

VADM Jan Tighe, USN
Commander, Fleet Cyber Command and U.S. 10th Fleet

The Honorable R. James Woolsey
Former Director of Central Intelligence

Jeff Wright
Consultant, CACI International Inc

Mr. Wright also served as Program Manager and Advisor

Advisors

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

Michael Dolim
Executive Director, Association of Old Crows

Donald Fulop
Executive Vice President, Business Development, CACI International

Hilary Hageman
Vice President, Deputy General Counsel, CACI International Inc

Z. Selin Hur
Strategic Program Principal, CACI International Inc

Jake Jacoby
Executive Vice President, Strategic Advisor for Intelligence Business
CACI International Inc

Ben Lerner
Vice President, Center for Security Policy

Anthony Lisuzzo
Director, Association of Old Crows

William Philbin
Senior Vice President, Center for Security Policy

Symposium Founders

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

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

Publisher and Editor-in-Chief

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

Event Manager

Erica Davis
Marketing Administrator,
CACI International Inc

Participant Coordinator

Casey Pierce
Business Analyst,
CACI International Inc

Report Lead

Charles Rice
Technical Writer,
CACI International Inc

Editors

Michael Pino
Publications Principal,
CACI International Inc

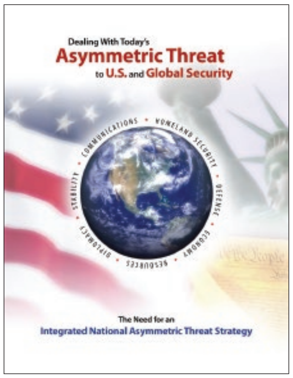
Ken E. Israel
Technical Writer,
CACI International Inc

Art Direction & Graphic Design

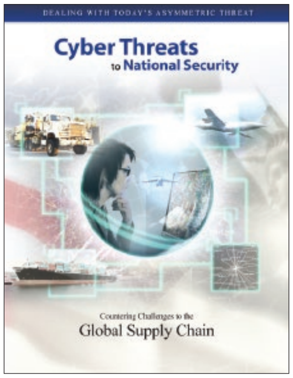
Stephen Gibson
Creative Director,
CACI International Inc

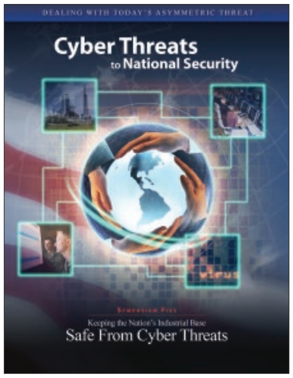
Find downloadable reports from all symposia in the three series at The Asymmetric Threat website **(asymmetricthreat.net)**.

SERIES ONE – Asymmetric Threats to U.S. and Global Security

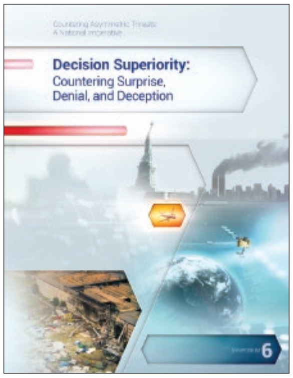

Dealing With Today's
Asymmetric Threat
to U.S. and Global Security
The Need for an
Integrated National Asymmetric Threat Strategy

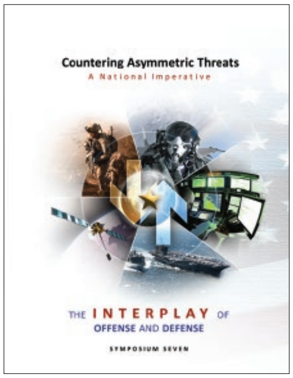
SERIES TWO – Cyber Threats to National Security

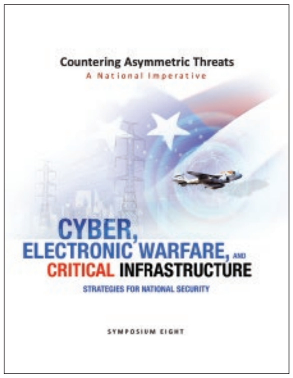

DEALING WITH TODAY'S ASYMMETRIC THREAT
Cyber Threats
to National Security
Countering Challenges to the
Global Supply Chain

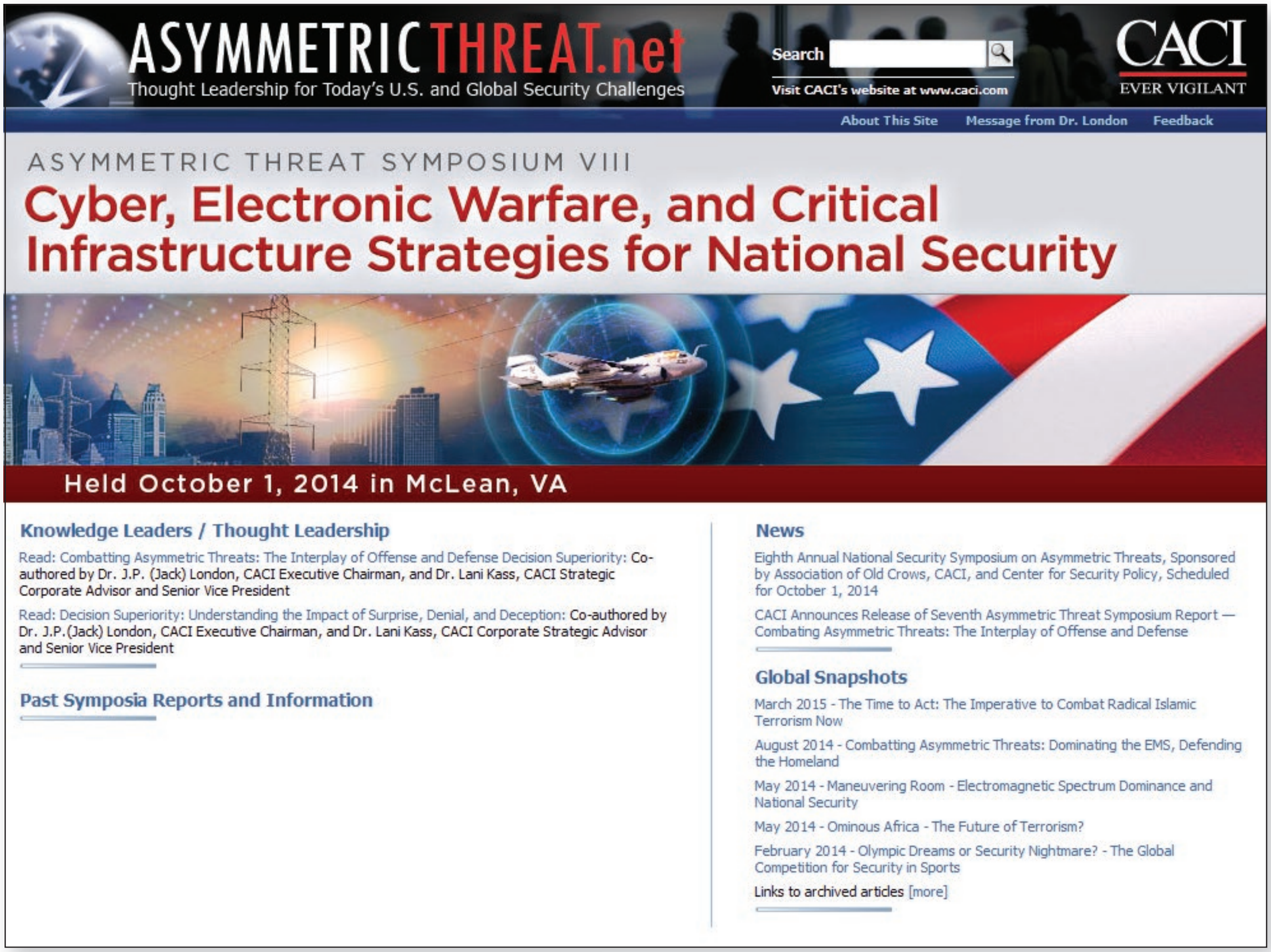

DEALING WITH TODAY'S ASYMMETRIC THREAT
Cyber Threats
to National Security
Keeping the Nation's Industrial Base
Safe From Cyber Threats

SERIES THREE – Countering Asymmetric Threats: A National Imperative









ASYMMETRICTHREAT.net

Thought Leadership for Today's U.S. and Global Security Challenges

Search

Visit CACI's website at www.caci.com

CACI

EVER VIGILANT

About This Site · Message from Dr. London · Feedback

ASYMMETRIC THREAT SYMPOSIUM VIII

Cyber, Electronic Warfare, and Critical Infrastructure Strategies for National Security

Held October 1, 2014 in McLean, VA

Knowledge Leaders / Thought Leadership

Read: Combatting Asymmetric Threats: The Interplay of Offense and Defense Decision Superiority: Co-authored by Dr. J.P. (Jack) London, CACI Executive Chairman, and Dr. Lani Kass, CACI Strategic Corporate Advisor and Senior Vice President

Read: Decision Superiority: Understanding the Impact of Surprise, Denial, and Deception: Co-authored by Dr. J.P.(Jack) London, CACI Executive Chairman, and Dr. Lani Kass, CACI Corporate Strategic Advisor and Senior Vice President

Past Symposia Reports and Information

News

Eighth Annual National Security Symposium on Asymmetric Threats, Sponsored by Association of Old Crows, CACI, and Center for Security Policy, Scheduled for October 1, 2014

CACI Announces Release of Seventh Asymmetric Threat Symposium Report — Combating Asymmetric Threats: The Interplay of Offense and Defense

Global Snapshots

March 2015 - The Time to Act: The Imperative to Combat Radical Islamic Terrorism Now

August 2014 - Combatting Asymmetric Threats: Dominating the EMS, Defending the Homeland

May 2014 - Maneuvering Room - Electromagnetic Spectrum Dominance and National Security

May 2014 - Ominous Africa - The Future of Terrorism?

February 2014 - Olympic Dreams or Security Nightmare? - The Global Competition for Security in Sports

Links to archived articles [more]

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.

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.

ASSOCIATION OF OLD CROWS 1964-2014

CENTER FOR SECURITY POLICY

CACI EVER VIGILANT

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

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

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

asymmetricthreat.net

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

©CACI 2015