Cyber Threats to National Security

Countering Challenges to the Global Supply Chain

This document is intended only as a summary of the personal remarks made by participants at the March 2, 2010 symposium, "Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain," co-sponsored by CACI International Inc (CACI) and the U.S. Naval Institute (USNI). It is published as a public service. It does not necessarily reflect the views of CACI, USNI, the U.S. government, or their officers and employees.

July 2010

Contents

Executive Summary

The United States is faced with an unprecedented asymmetric threat to its national security, one to which the public is not yet fully awake. Of increasing importance, it is a threat to the nation's vast information assets, networks, and systems that operate in cyberspace. Within this context, it is critical to look at the cyber threat to the nation's supply chains.

Assessing the Cyber Threat

Cyber threats are asymmetric because attacks may be perpetrated by the few upon the many, with little cost and resources. Cyber attacks are typically anonymous, launched from any of billions of sources worldwide. Impacts may be immediate and obvious, or dormant and subtle, eluding recognition for years. Degrees of damage can range from inconvenient downtime of personal systems to the life-threatening destruction of critical infrastructures.

Cyber threats are growing and will impact everyone. The increasing global dependence on technology has only increased vulnerability to it. In turn, increased connectivity has exacerbated existing security threats. Developing an effective and comprehensive national cybersecurity strategy to counter these threats is paramount.

A key component of this strategy will be a capability to protect U.S. supply chains from mounting cyber threats. Supply chains provide goods and services that are essential to the functions of the U.S. government and its economy, the well-being of Americans, and the support and protection of American troops worldwide.

Securing Supply Chains

Historically, U.S. supply chains have been largely immune to threat because the most critical supply chains were internal to North America, far from the influence of foreign actors. This is no longer true in the cyber age.

During the last 25 years, globalization has increasingly compromised U.S. supply chain immunity. The worldwide cyber domain has also become increasingly essential to every aspect of governmental, commercial, and personal life. U.S. communications, command, and control technologies and capabilities have become inextricably interwoven with those of every nation, both friendly and hostile to U.S. interests.

In the cyber age, the nature of the supply chain must be reexamined. The vast majority of U.S. supply chains rely on information technologies to carry out their functions and processes. At the same time, the convergence of computer and communications technologies potentially compromises every information system worldwide. Threats to both private and government supply chains are equally affected.

Even as cyber threats mount, it is also clear that solutions to these threats also reside in the cyber domain. Technologies that can be turned against a nation can also be the source of its defense. The U.S. must commit time, funding, and expertise to fully exploring this aspect of cyberspace.

The Way Forward

To enforce cybersecurity of U.S. supply chains, it is necessary for the government and its citizens to engage in a unique collaborative effort. Every user of a cyber-enabled device has in their hands a point of vulnerability and a source of potential attack, and is a potential cyber warrior.

Congress and the executive branch must engage cooperatively in defining roles and responsibilities. Diplomatic solutions must be explored, and a public-private partnership must develop. Responsibility must be shared among the government, the private sector, and every private citizen to protect U.S. cyber assets.

Recommendations

A number of recommendations may be made to advance the national understanding of cyber threats in general and supply chain threats in particular. The U.S. must:

1. Ensure the nation is prepared to react to and preempt cyber attacks;
2. Make supply chain security part of the establishment of an overall cyber intelligence capability;
3. Develop the ability to build a limited number of computer and communication systems that are absolutely certain to be secure; and
4. Carry out a sustained strategic communications campaign to provide the public with a realistic appreciation of the cyber threat.

1 Introduction

As the United States government develops strategies that address the diversity of twenty-first century asymmetric threats, CACI International Inc, along with the National Defense University (NDU) and the U.S. Naval Institute (USNI), organized and presented a series of *pro bono* symposia to contribute to the national discourse on this topic.[1] These symposia examined and defined the asymmetric threat; explored the key elements of a revised national security strategy; and helped articulate the framework for implementing "smart power" – the balanced synthesis of hard and soft power.

A new symposium series has now begun on the topic of cyber threats. The first in this series, *Cyber Threats to National Security – Countering Challenges to the Global Supply Chain*, was co-sponsored by CACI and USNI on March 2, 2010. It addressed emerging threats in cyberspace, with a focus on national supply chains. This report presents a summary of the discussions, findings, and recommendations from that symposium.

The convergence of communications and computer technologies has brought with it the unprecedented potential to undermine U.S. national security through cyber attacks at any point in the global cyber domain. Graphic courtesy of CACI.

1 NDU co-sponsored the first symposium on asymmetric threats and USNI co-sponsored the second two, concluding the series at three. Published reports from these symposia can be found at http://asymmetricthreat.net.

1.1 An Unprecedented Asymmetric Threat

The U.S. is faced with a great strategic reversal, one with asymmetric roots grounded in the birth of the cyber age. Although there is much recognition of the cyber revolution that has swept the world in recent years, the strategic reversal has yet to gain broad public appreciation. Like the boiled frog of urban legend, the U.S. is in increasingly hot water but has not yet fully awakened to its predicament.

The idea that cyber attack is an increasing threat to the U.S. ability to pursue its national security objectives, at both the strategic and tactical levels, emerged in the late 1990s. That the cyber threat might be a threat to the success of the nation, however, is not yet broadly recognized in American society.[2] The first Gilmore Commission Report in 1998 had the briefest mention of the cyber threat; the 2000 report included much more.[3]

One of the greatest challenges facing the national security community is communicating the significance of this threat to the broader U.S. society. The cyber threat does not fit cultural stereotypes associated with past threats. The problem is exemplified by the continuing controversy over the treatment of captured terrorists: are they warriors to be subjected to military justice, or are they criminals to be subjected to civilian justice? Now consider how difficult it may be to properly respond to a threat created by a "techie," or even a "tech squad," half a world away.

U.S. warfighting and national security prowess have relied on the power and remoteness of its industrial base, secure internal lines of communications, and overwhelming logistics power.[4] Today, the convergence of computer and communications technologies has brought America's remotest regions into a cyber domain in which everything is potentially connected at the speed of light. Now and for the foreseeable future, cyber attack, when integrated with hard and soft power, can threaten America's national security in ways that are truly unprecedented. This has profound implications for America's strategic posture.

2 Steven Chabinsky, CACI-USNI symposium comments.
3 Hon. James Gilmore, CACI-USNI symposium comments.
4 General William Wallace, CACI-USNI symposium comments.

"Cybersecurity has the same reach as homeland security. It touches everything."

– Former Secretary of Homeland Security Tom Ridge

Cybersecurity plans and programs have been developed by the government and have been discussed in industry for decades. Exacerbating traditional security threats, the cyber component adds a genuinely new dimension that obscures the threats and makes the need for action less obvious. Consequently, the political will to implement these plans and programs has not been fully marshaled. America's response to the cyber threat has not been to a level that counters the actions and investments of other nation states and cyber threat actors.

In the early 2000s, there were several high-level efforts to elevate the cybersecurity discussion to the national level. The Department of Homeland Security (DHS) began development of a national cyber strategy, which laid out a plan for dealing with cyber crime and terrorism. Among other initiatives, the Department of Defense (DoD) established the DoD Cyber Crime Center in October 2001. However, while there was progress toward an approach to incorporate cybersecurity into the national psyche, the threat of cyber attacks remained an esoteric concept that was not fully comprehensible to most of U.S. society.

This conceptual divide was further deepened by the terrorist attacks of September 11th. National attention turned to the immediate fear that terrorist organizations could physically attack the United States and its citizens. Protecting ports of entry and territorial boundaries became paramount. Meanwhile, those who saw cyberspace as a means to achieve their ends continued to develop capabilities and planned for the eventual use of cyberspace as a weapon.

A comprehensive national strategy that effectively addresses the cyber threat remains to be developed. The U.S. has had innumerable tactical successes, but the window to develop and implement a national strategy is closing and may not remain open much longer. If another decade passes without such a strategy, the nation may not survive the threat.[5]

5 Chabinsky, op. cit.

1.2 The Cyber Challenge to U.S. National Supply Chains

The shaping of a U.S. response to cyber threats requires a strong focus on a key vulnerability: U.S. supply chains.

A supply chain is a system of organizations, people, processes, technology, information, and resources. It is organized to enable suppliers to develop raw material and natural resources into finished products, and then deliver goods to their customers. An end-to-end process from raw materials to finished goods, the supply chain faces constant threats at every step.

U.S. supply chains are threatened as never before. Historically, supply chains were largely immune to attack because the most critical processes were internal, far from the influence of foreign threats. The country's continental span afforded significant supply chain protection.

In the last 25 years, however, U.S. supply chain immunity has been compromised. A worldwide cyber domain has been created in which U.S. communications, command, and control circuits are interwoven with those of friend and foe alike. Through both independent and integrated cyber attacks and other asymmetric means, U.S. supply chains may be at greater risk of significant disruption than at any point since the Civil War.

Asymmetric strategies to disrupt or destroy an adversary's supply chain operations have long been fundamental to U.S. warfighting strategy, one that few adversaries could effectively counter. Likewise, protection of American industrial capacity and supply chains has been a fundamental national priority.

Today, the tables have turned on the U.S. To some extent, this has been a result of unintended consequences of its own actions in developing and globalizing Internet technologies. The global reach of the Internet and the pervasive interconnection of government and non-governmental networks leave the U.S. open to a variety of cyber attacks. This includes "cyber manipulation," which is any information operation that results in a compromise of the service or product delivered through a supply chain.

Large container ships must not only be physically protected but also safeguarded from cyber attacks that could disrupt scheduling and delivery of vital goods. Image in public domain.

Consequently, there are countless weak links in supply chains associated with computer and communications technologies. U.S. adversaries often pick the supply chain as the first attack vector against the U.S. This may involve weak points in hardware, software, the architecture of the Internet, or other communications infrastructures that include those used by mobile devices.[6]

Furthermore, all aspects of supply chains are subject to cyber attack or manipulation, including design, manufacturing, transport and delivery, installation, and repair or upgrade.[7] There are also numerous avenues through which attack or manipulation can be carried out.

Computer and communications supply chains are the one thing shared in common by all other supply chains. In effect, they are the "supply chain of supply chains." Nearly all supply chains are dependent on converged computer and communications technologies. If these are compromised, then all supply chains are compromised, whether they are known to have been attacked or not. Furthermore, since the computer and communications technologies have replaced their predecessors around the world, every supply chain everywhere is, in principle, compromised. Currently, supply chain users around the world lack the hardware or software assurance technologies and business processes necessary to have a better security environment.[8]

The U.S. government, which sponsored the development and application of virtually all the technology innovations that led to the information technology mass market, itself lacks the resources to address the cyber threat in a meaningful way.

While the U.S. government is a large user, perhaps arguably the largest single user, of converged computer and communications technologies, it is not a big user on the global scale. For example, a single software product like Microsoft Windows® sells at least 100 million units a year, but sales to the U.S. government are likely to be less than 10 percent of annual sales. Therefore, industry won't change its technology or processes for a U.S. government agency unless the government pays for the change.[9]

In addition to the sheer scale of global market forces, the influence of the U.S. government is diluted by social and political forces. The boundaries between countries, companies, and individuals have grown indistinct. Conflicting loyalties may thwart U.S. goals. What happens when the U.S. government deals with global suppliers and makes requests based on national security interests – and other governments ask for security modifications that conflict with U.S. requests?[10]

In short, there is a growing threat of cyber attacks, especially to U.S. and global supply chains. The reality of this must become part of both U.S. policy and public perception.

1.3 National Response to the Threat

The scale, scope, novelty, and complexity of cyber threats demand an application of all the instruments of national power, both public and private, if the U.S. is to respond successfully.

6 Chabinsky and Vergle Gipson, CACI-USNI symposium comments.
7 Chabinsky, op. cit.
8 Ibid.
9 Zalmai Azmi, CACI-USNI symposium comments.
10 Bruce McConnell, CACI-USNI symposium comments.

The lead role in developing and enacting U.S. cybersecurity policy is shared by the legislative and executive branches of government. A concerted response by these branches will strengthen legal authorities, establish and clarify roles and responsibilities, and change public perceptions.

Congress must consider a number of factors in enacting legislation specifically focused on improving cybersecurity. It must establish a U.S. capability to monitor emerging technologies and rapidly respond to threats from any source. It must tailor legislation to the executive agencies in which these capabilities will reside and be implemented. Budget constraints must be considered, while Constitutional limits of federal power and the rights of local and state governments are respected. Privacy and other individual rights also must not be infringed.

The President must continue to make cybersecurity a national priority, and executive branch policy must clarify and define agency roles and responsibilities. Executive policy should include increasing efforts to define a common and clearly understood lexicon of cyber domain and cybersecurity terminology. Presidential guidance and directives will continue to be vital in helping federal agencies establish complementary and collaborative strengths in supporting U.S. national security.

Because cyber threats are international in scale and scope, global coordination and cooperation are essential. The executive branch must therefore also formulate and execute diplomatic initiatives complementary to domestic actions.

The government also needs to work closely with the private sector for a truly comprehensive cyber response. The private sector is the source of most cyber technologies and products and owner of many of the systems under greatest threat.

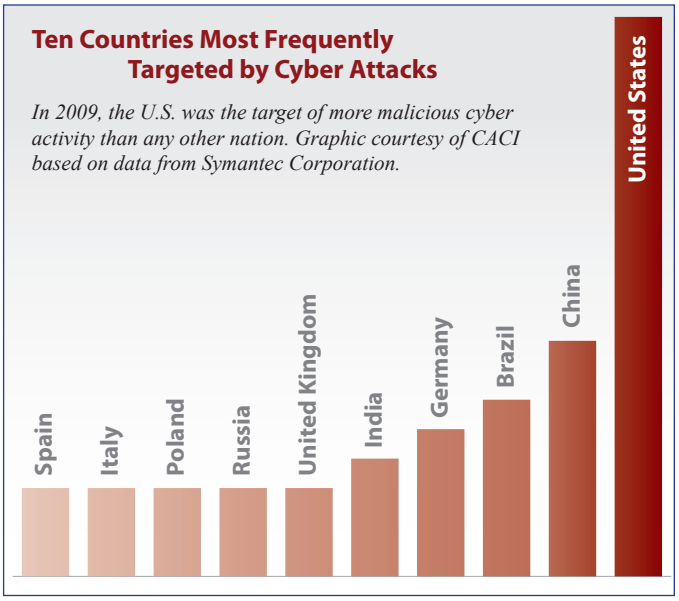
Finally, the government must commit to a strategic communications initiative that ensures every American understands the true nature of cyber threats and takes a personal stake in cybersecurity. Only when the public is fully informed, and acting on that knowledge, can government initiatives truly move forward.

2 Assessing the Cyber Threat

Looking at the cyber threat environment, it is clear that adversaries of the U.S. have compromised the nation's interests. The computers of the nation's own citizens are infected with malicious software and unwittingly being used against U.S. interests. The federal government is constantly under attack. U.S. critical infrastructure is being targeted and explored by adversaries on a daily basis.[11]

The Center for Strategic and International Studies (CSIS) found that more than 50 percent of businesses operating critical infrastructure, including electrical grids and gas and oil supplies, have experienced cyber attacks at a cost of millions of dollars each day, posing a significant threat to essential services.[12]

While the U.S. has been preoccupied discussing the implications of security in the modern, connected, high-bandwidth world, its adversaries have been busy developing exploitative technologies and learning



11 According to the security software maker Symantec, in 2009, for the second year in a row the U.S. was the victim of more malicious cyber activity than any other country in the world, suffering 19 percent of all global attacks. See *Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV*, published April 2010.
12 Hon. Tom Ridge, CACI-USNI symposium comments.

from experience. They are fully capable of operating offensively within cyberspace. The globalization of manufacturing products in the information and communications sectors means that the U.S. and other highly developed countries, including all the G20 members, are dependent on newly emerging producers of technology in this space.

The U.S. now finds itself more reliant than ever on converged computer and communications technologies, more so than almost any other country. While benefiting from the efficiencies these technologies bring, the U.S. is simultaneously in an increasingly defensive posture with adversaries that have identified cyber warfare as the new asymmetric weapon of choice.

America's adversaries have come to realize that the very efficiencies provided by information technology, the very technologies that enable all modern societies to thrive, can also be used to efficiently undermine U.S. security.

2.1 The Realities of the Growing Cyber Threat

The battlespace has changed. Notwithstanding Sun Tzu's recommendation to "know thy enemy," the U.S. is no longer dealing with a single known enemy, or even a handful of known enemies, on known battlefields.[13]

Instead, the U.S. is dealing with hundreds, even thousands, of attacks daily. They come from known and unknown adversaries, attacking from multiple entry points. Attacks can come from solitary hackers, inside and outside the network, inside and outside U.S. borders, and be intentional as well as unintentional. There are also large-scale, coordinated attacks from friendly and unfriendly countries all over the globe.

The highest rate of cyber attacks on U.S. networks – perhaps surprisingly – is from within the United States. China is second, and Spain is third.[14]

These attacks are manifested in the form of system crashes, denials of service, counterfeiting, corrupted or stolen data, material theft, delivery delays, and misdirected service. They can be obvious, immediately identified events; backdoors that become effective only when a specific set of events occurs in the future; or events that are timed to occur in the future. Not only can these attacks immediately disrupt the flow of the goods and services to the warfighter, they can also take down entire networks.

By 2017, it is expected that Chinese investment in information technology will surpass that of the U.S. by 5 percent.[15] What are U.S. institutions doing to counter this threat? How can DoD develop awareness of the cyber threat in its training, war gaming, simulation, and officer development?

2.1.1 The Highly Asymmetric Nature of Cyber Threats

During the 1990s, the growing prominence of the information technology mass market and the Internet drew increasing attention to the potential for and emergence of new forms of asymmetrical warfare. Experts began to recognize that converged, networked information technology and communications systems reinforced other technical advances to empower individuals and small groups in unprecedented ways that could challenge even the power of the United States.[16]

Cyber actors, from individuals, to criminal groups, to rogue states and terrorists, can today easily combine to launch a customized cyber threat.

- Individuals. At the lowest end of the threat spectrum are uncoordinated individuals acting on their own. Although some individual actors are highly intelligent and may pose a risk to systems, their motivation is often limited to achieving personal satisfaction or recognition based on the disruption they hope to cause. The limited level of resources available to individuals reduces the risk posed by this class of threat.

13 Azmi, op. cit.
14 Ibid.
15 Ibid.
16 Among the analyses that first recognized these possibilities are John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information Age Terrorism," in Zalmay Khalilzad, John P. White, Andrew W. Marshall (eds.), *The Changing Role of Information in Warfare* (Santa Monica, CA: RAND Corporation, 1999); and Martin Shubik, "Terrorism, Technology and the Socioeconomics of Death," *Comparative Strategy*, 1997.

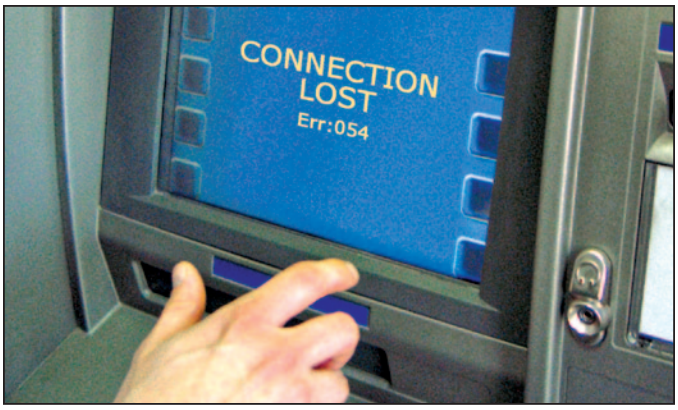
- Corporations. Industrial espionage has developed in cyberspace as a way to maximize investment – or deny others the fruit of their efforts. Whether conducted by otherwise legitimate corporations, or any of the other classes of cyber actors mentioned here, industrial espionage undermines fair business practices and is often supported by nation states as a means to advance their societal capabilities and industrial base with little investment. Corporate actors are also difficult to pin down because assets may be compromised from both inside and outside the corporation.

- Criminals and Criminal Enterprises. Many threats in cyberspace are motivated by personal financial gain or related to criminal acts of vandalism. Criminals and criminal enterprises within cyberspace have become more organized, including highly organized rings that traffic in personal information, credit cards, identities, and other information with value. In many cases, criminal software and hardware development capabilities rival those of software and hardware industry leaders.

- Terrorists. Because cyberspace offers anonymity, terrorist organizations have begun to use the Internet as a key tool to support recruitment, funding, and organization goals. Cyberspace provides an easy way to fund terrorist activities and transfer resources through anonymous online transactions. It also provides the means to transfer knowledge and provide command and control to support the terrorist organization. Unlike criminal enterprises, because motivations are not driven entirely by greed, terrorist activities are more difficult to counter.

- Nation States. Nation states have long recognized the value of information systems as critical elements of good governance practice, but they have also been used to subvert other nation states' security. In the national security arena, computing systems have long been used to break encrypted messages and disrupt communications and command and control systems. Because identities are difficult to trace in the cyber domain, it is difficult to determine the nation state behind a given attack.

As far as these cyber actors are concerned, the same converged computer and communications technologies that enable any cyber threat also facilitate a virtual cyber-summit. In the anonymity of cyberspace, common cause can be found, plans made, and actions coordinated and taken. The attackers may have never met in person, before, during, or after the attack. Attacks can be directed against individuals, corporations, governments, or against any combination thereof.



Are Americans ready for cyber attacks that can disrupt the delivery of essential goods and services? Graphic courtesy of CACI.

A commonly used mechanism to describe the degree to which a system is vulnerable is to describe the "surface area" that is exposed to threat. With the many systems connected to the Internet, cyberspace exposes a vast surface area with innumerable vulnerabilities that a threat may exploit.

There are literally billions of points from which an attack can be launched using ordinary technology available almost anywhere to anyone. Any software technology that cannot be found for download on the Internet can be obtained through black or gray market channels. Other assets, like botnets, can be rented over the Internet.[17]

The asymmetries of converged computer and communications technologies available to cyber actors are especially striking. Beyond an Internet-connected computer, the cyber attackers' marginal technical and operational resource requirements are low. The barriers of entry to cyber actors at all levels of organization are low. The cost of exploits is low. The cost of launching attacks is low. The cost of failure or getting caught is also low.

17 A botnet ("robot network") may be described as a collection of networked and compromised computers under the remote command and control of a criminal adversary. "Over 1 Million Potential Victims of Botnet Cyber Crime," FBI Press Release, June 13, 2007. Accessed at http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm on May 25, 2010.

As society becomes better at protecting information technology assets, attackers will look to identify more cost-effective means to carry out their attacks. In the case of specific, well-protected systems, attackers may already be looking to the supply chain as a potential vulnerability vector. For a nation state, targeting an individual supply chain of a weapons system or a system not connected to the Internet may be the only cost-effective way to affect the balance of power in its favor.

Consider the following scenario. In order to target a specific system, the attacker must generally do one of two things: identify vulnerabilities to establish a foothold and gain privileged access to the computing resources of the system, or overload the system to cause it to malfunction.

Ubiquitous vulnerabilities present a great opportunity to disrupt systems. The majority of vulnerable systems in cyberspace are personal workstations or other systems that have limited value, except to the individual that regularly uses the computer.

However, attackers have found ingenious ways to exploit these low-value computers. Attackers aggregate large groups of such computers into botnets that can be used to overload systems. The development of botnets by an attacker also may be a preliminary stage of a larger attack to come.

The amount of damage that can be done by a cyber attack is, then, highly likely to be greater than the cost of the resources required to plan, develop, and execute the attack. While attacks on specific, well-protected systems may require a much larger investment and may be less asymmetric, cyber attacks generally tend to be highly asymmetric, offering attackers an extremely high return on their investment.

Among other important asymmetries associated with the cyber threat are these:

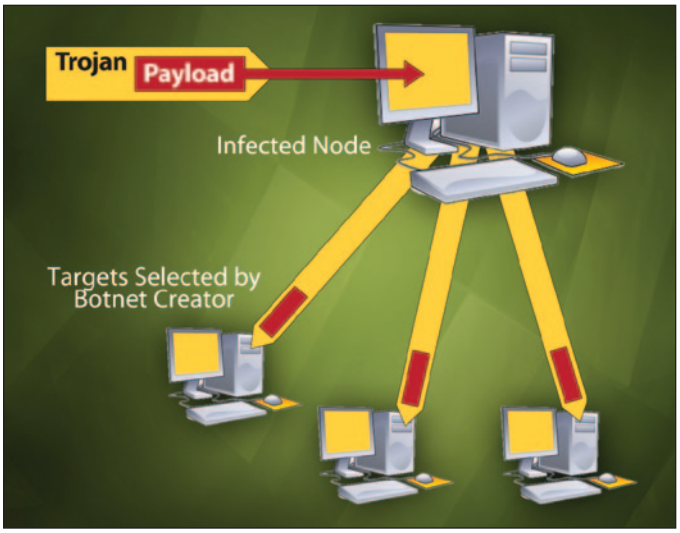
- Defenders need to be successful always and everywhere, usually at high cost, while attackers need to be successful only occasionally.
- Governments are slow to respond, lacking agility compared with asymmetric cyber actors.
- The pace of technical change is great and funded by the ever-growing mass market.
- There are asymmetries in the education needed to attack/manipulate vs. protect and defend due to the easy availability of technologies in the global marketplace.
- There are major cost asymmetries.[18]

The highly opportunistic and enigmatic nature of cyber threats is unlikely to change any time soon.

2.2 Cyber Threats Affect Everyone

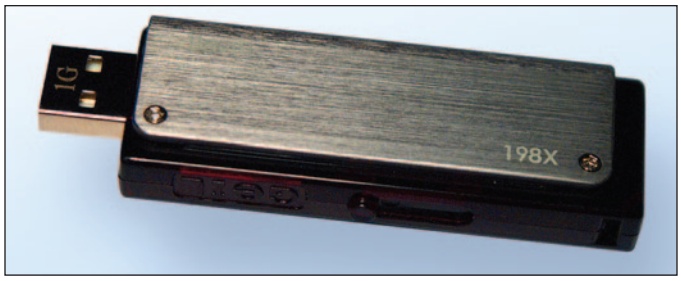
It is clear that the impact of an attack through and on cyberspace will affect all aspects of society. Modern societies are dependent on technology in general and cyberspace in particular for providing safety and security through the effective delivery of essential goods and services.

Cyberspace also has become an enabling medium for communications within society and between the government and constituents. As modern society develops, additional cyber capabilities will be adopted, including electronic voting and other technical processes that will be critical to society's function in ways that may be unimaginable today.



Criminal-controlled robot networks, or "botnets," in which computers are infected with malicious software that allows them to be controlled by a remote operator, represent a growing cybersecurity threat. Graphic courtesy of CACI.

18 For example, consider the recent disclosure that unencrypted video signals from American unmanned aerial vehicles (UAVs) have been intercepted with software available over the Internet for less than $30. The cost of retrofitting the UAVs with encryption technology is much greater.



Malicious code secretly built into a single thumb drive can take down an entire network. Image in public domain.

Today's world of ever-increasing efficiency is driven by the automation and connectivity provided by cyberspace. Just as automation and advanced technology in agriculture improved methods of meeting the needs of a growing population, the automation provided by information technology allows society to meet the needs of a larger population.

The question is whether society can tolerate the loss of automation capabilities for an extended period of time. In many ways, the current culture of the United States has not developed a fully informed appreciation of the potential effects of a cyber attack on critical social processes. Like the transformation in awareness of the reality of terrorism between September 10th and 11th, American opinion is in many ways yet to be formed regarding the consequences of, and responses to, a major cyber attack.

2.2.1 Impact on Government

Attacks on government generally take two main forms.

Direct attacks on national security seek to undermine government by degrading its ability to ensure the safety and security of its constituents. Typically, adversaries seek to attack critical systems and government functions to destroy society directly. These attacks may also prevent the U.S. military from communicating with units in battle zones or affect the ability to direct an attack by certain remote assets.

Indirect attacks on government manipulate messages or government information to undermine trust in that government held by citizens, other governments, and non-governmental organizations. Attacks of this nature may disrupt or subvert regular programming with threatening messages. These types of attacks seek to affect the morale of society through diffuse attacks on less-than-critical functions. Government must establish effective programs and processes to counter the effects of both types of attacks.

2.2.2 Impact on the Private Sector

The private sector plays a key role in cybersecurity and the security of supply chains. Not only does the private sector own and operate 90 percent of the critical infrastructure, it manages and operates the vast majority of the information technology supply chain and other supply chains supporting the United States. Cyber attacks on the private sector therefore impact society very broadly.

At the same time, the government has less leverage in requiring private sector entities to maintain secure cyber infrastructures, at least compared to government control of its own departments and agencies. Protecting commercial cyberspace may require greater controls, as well as incentives, than are currently in place.

One important issue is the amount of high-end technology devices produced overseas, particularly in China and other emerging markets. Many basic communications devices, like handheld radios, may soon no longer be available from U.S. manufacturers. Thumb drives made overseas may contain unwanted and potentially infected software.

Outsourcing data centers to locations abroad is another questionable practice. It is of great concern that vast amounts of U.S. data are stored or routed by overseas facilities. This makes vigorous risk mitigation strategies and actions even more important in the existing threat environment.

2.2.3 Impact on Individuals

Individual computer users play an increasing and highly critical role within the cybersecurity environment.

Because the U.S. population owns the largest share of converged computer and communications technologies in the world, U.S. citizens possess a large pool of potentially vulnerable systems that may be surreptitiously co-opted by botnets. This kind of exploitation increases the complexity of conceptualizing and dealing with cyber attacks because these botnets may be located within U.S. territorial boundaries and owned by U.S. citizens.

Everyone who sits in front of a PC, or uses a smart phone or other Internet-enabled device, is a potential cyber warrior. Individuals are either an asset or a liability to the security of the systems they and everyone else utilize, whether in their personal capacity or in their public capacity as an employee of an organization, a student in an educational institution, or in any other societal role.

That each user may be a cyber warrior is not a matter of dramatic license: it is literally true and easily demonstrable. The recent breaches of Google's infrastructure have been reported as having originated with a single Google employee in China who, according to press reports, clicked "on a link and connect[ed] to a 'poisoned' web site" and "inadvertently permitted the intruders to gain access to his (or her) personal computer and then to the computers of a critical group of software developers at Google's headquarters in Mountain View, Calif."[19]

2.2.4 Impacts at the International Scale

The recent breaches of Google's infrastructure are a powerful reminder that converged computer and communications technologies are international in scope. This is both because of globalized businesses like Google, but primarily because the main value of these technologies is gained when they are connected together in cyberspace.

Some of the greatest expressions of the cyber threat have been seen in international venues. The attacks against Estonia in the spring of 2007 illustrate the extent of international cybersecurity issues. Estonia's Internet infrastructure was attacked, causing the country's numerous Internet-dependent citizens problems in carrying out financial transactions, and preventing the government from carrying out certain governmental functions.

The consequence is that the impacts on government, industry, and individuals are replicated in every part of the world, wherever cyberspace has been extended. The exact scope of the benefits of cyberspace, as well as the threats, varies from locale to locale. In some regions a particular benefit or threat is enhanced, diminished, or absent, but the overall pattern is invariant.

19 John Markoff, "Cyberattack on Google Said to Hit Password System," *New York Times*, April 19, 2010.

3 Securing Supply Chains in the Cyber World

Today's supply chains commonly encompass multi-modal and globalized distribution systems.

Supply chains exist within specific marketplaces that are defined by customer needs, supplier capabilities, and applicable regulatory requirements. Many involve critical infrastructures or other sensitive products or services, making it imperative that at every point, repeatable and acceptable controls ensure the integrity of the materials being procured, produced, and distributed. Supply chains themselves can be used to transport threats or carry out attacks by adversaries.

It is critical that supply chains be prevented from being used as amplifiers or enablers for integrated or faceted attacks. The interrelationships and dependencies between supply chains for critical infrastructure and other areas must be well understood.

3.1 Supply Chain Threats and Vulnerabilities

Supply chain security is generally defined in terms of assured storage and delivery of physical and digital goods and services. Yet there is much more to it. It is also the application of governance and controls that ensure the integrity of the supply chain business process, as well as the material and products in the supply chain. It uses technical and procedural controls to protect the confidentiality, integrity, and availability of supply chain systems, processes, and information.

"In the modern world, the supply chain is information. When something has been ordered ... where it's going to be manufactured and by whom and how much and what specifications ... all are either on the Internet or in private data systems that are subject to being hacked and invaded."

– Former Virginia Governor James S. Gilmore, III

U.S. troops unloading supplies and equipment in southern Afghanistan. Every step of the supply chain must be secured to prevent asymmetric threats from targeting resources that protect and serve U.S. warfighters. Photo courtesy of Air National Guard.

In protecting the supply chain, it is critical to understand the value of both what passes through the supply chain as well as the information managed by the supply chain. Technical information, intellectual property, and production methods must be protected. Because industrial espionage targets this type of information, it is necessary to ensure there is no leakage of technical information. The unauthorized modification of technical details can affect the integrity of the products being delivered.

Protection of supply chain processes is also critical. Because the knowledge of the supply chain workflows, functions, review techniques, sampling and audit capabilities, and risk management controls can be use to prosecute effective attacks, processes must be protected from disclosure. Additionally, the visibility of partner information must be balanced with the risks associated with its release. An adversary targeting partners upstream can have serious consequences for the integrity of the end product.

How do the U.S. government and the U.S. as a whole allocate resources to assure supply chain security? What is the biggest risk? Today, the greatest vulnerability may be that U.S. supply chains are fragmented.[20]

20 Lieutenant General Claude "Chris" Christianson, CACI-USNI symposium comments.

There are very few acquisition systems that track an end item completely through the supply chain, whether it is the raw materials that electronic components are made from, the printed circuit boards that are assembled from the electronic components, or the electronic components that make up a sub-system. Most program offices, manufacturers, and vendors see their responsibility as taking material from their supplier, performing the operations that they are (contractually or officially) responsible for, and delivering that product to the next stage in the supply chain.

Rather than a global systems assessment, the practical expedient is that the component has simply to work, to perform as expected. The group that manufactures silicon chips usually does not know, or really care, whether the chips are going into a low-power radar amplifier or a high-speed computer, as long as they pass their factory acceptance test. The manufacturer has little interest if a box of silicon chips sits unguarded in a railroad siding for three weeks. As long as it gets to the next producer in the supply chain by the contractual delivery date, the chip manufacturer and their customer are content.

The same is true for the manufacturer of the low-power amplifier. Along the supply chain, no one may know or care if the amplifier is going on a ship, an airplane, or a land-based station. No great importance is attached to the fate of this amplifier once it passes the factory acceptance test and is delivered to the radar manufacturer in accordance with the terms and conditions of the subcontract.

The fundamental problem is that there are very few individuals or companies that focus on the global end-to-end requirements or security of the supply chain. Components of all scales are usually considered fungible and, consequently, most suppliers are not paid for ensuring all aspects of quality and security as described here. That degree of oversight is most often neither contractually nor culturally their job or their responsibility.

Absent detailed, objective knowledge of the entire chain, if there is no assessment of the security of all the suppliers, customers, interfaces, and every link in the chain, it is not possible to truly know where security investment dollars are going. Very few organizations assess the entire chain for weaknesses, analyze the results, or support a common outcome.

3.2 Securing the Supply Chain

Protecting supply chains will require a widespread effort. While the challenge seems daunting, there are several opportunities available.

Each element in the supply chain must be examined in a consistent, objective fashion, and the resulting data must be analyzed to determine its status relative to other elements to create a common picture. Supply chain networks should be designed to maximize their dependence on technology for their resilience, minimizing reliance on human interventions. This is desirable since there are too few people to respond quickly enough to every attack.

To maintain resiliency in the face of a highly fluid cyber environment, and an only somewhat more stable physical environment, it is necessary to continually monitor and adjust the supply chain. Identifying and maintaining the high ground, not clearly defined in the cyber domain, requires a solution expressed in terms of Doctrine, Organization, Training, Material, Leader Development, Personnel, and Facilities (DOTMLPF).[21]

Establishing a supply chain in this manner permits the creation of a response framework based on the ISO 28000 series, the World Customs Organization, the Department of Homeland Security Customs Trade Partnership Against Terrorism, and similar standards and approaches.[22] It would be a series of supply chain supplier and customer conditions and risk assessments that allow for a structured assessment of processes and measurement standards. Performance would be measured and corrective actions taken where necessary.

This approach provides the additional benefit of increased efficiency because the time and resources necessary to inspect a trusted supplier's products would be minimized, while focus on products from uncertified suppliers would be maintained. The result would be reducing the cost and schedule of supply chain shipments where appropriate, while helping to ensure security of the right product, to the right place, at the right time.

As the U.S. becomes better at resisting the threat to cyberspace, the attackers will be forced into the supply chain to maintain return on investment. To ensure protection is in place to meet the trajectory of the supply chain threat, incentives must be provided to maintain focus on developing controls within the supply chain.

The financial services sector provides a good example of the level of effort required to manage these relationships. Service providers employ standardized mechanisms to transmit information on operational and security risk. They use standardized processes to continuously audit and assess the effectiveness of security controls. This provides early warning of emerging problems by creating visibility into risks in the operating environment.

An even better example comes from the identification of controls designed to drive up the costs to an adversary attacking the supply chain. When the cost of attack is greater than the cost of implementing controls, defenders realize a return on investment.

This use of the supply chain as a deterrent requires a change in perspective. Potential returns should be identified and prioritized to support deterrence efforts. Instead of viewing the supply chain as a target, it may be time to make it a useful control point in defending the national interest.

It is critical to have an appropriate high-level focus on the long-term strategic need for security within all aspects of the systems development lifecycle. A common language of supply chain security must also be developed. In many cases, there is a lack of technical underpinnings that support the communication of supply chain integrity information between partners within the supply chain.

3.2.1 The Information Technology Supply Chain

Threats to information systems security that originate from the Internet have consumed public attention. Yet it is safe to say that nothing in today's supply chain moves without electrons. Therefore, the security of supply chain technology is paramount.

The integrity of the supply chains that produce the converged computer and communications systems that support all other supply chains is absolutely essential to the integrity of products within each supply chain. If information technology supply chains are insecure, then

21 DOTMLPF refers to the standard set of factors to be considered by the military when establishing a new national security capability.
22 See the glossary for more information.

all other supply chains are insecure by inheritance. It is the link upon which all others depend.

However, when considering the threat to society, it is critical to focus on the threats to information systems and the components of information systems throughout their development lifecycle.

From the time raw materials are obtained to build hardware components, or when designs are drawn up for software, to the time the cyber systems are disposed of, they are under constant threat of manipulation or attack. Current cybersecurity efforts are focused primarily on governance and compliance efforts that seek to provide a base level of security for systems once implemented. The defect of this approach is that it does not account for the integrity of system components as they travel through the supply chain prior to procurement. Because the supply chain is now a complex, interlocked process, threats can originate from anywhere worldwide.

Some supply chains related to specific systems and components have been secured. They include those involved with development of weapons systems or that handle controlled or hazardous materials, such as nuclear and chemical materials. Unfortunately, there have been notable exceptions, including one of the Pentagon's most expensive weapons programs.[23]

Multiple solution sets must be in place to counter a myriad of cyber threats. Graphic courtesy of CACI.

23 Although many details about the attack were not released, attackers were able to download a significant amount of information related to the F-35 jet fighter. Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009.

Computer and communications supply chains are the "supply chain of supply chains." If information technology supply chains are compromised, all other supply chains are potentially compromised. Graphic courtesy of CACI.

Historically, however, supply chains that produce general information technology components have not incorporated controls to ensure the integrity of the information systems developed, even though they are the weapons of today's and tomorrow's cyber battlefield.

This simple reality is recognized by the Comprehensive National Cybersecurity Initiative (CNCI), which devotes an entire initiative to security of the information technology supply chain. In fact, CNCI-11 includes the requirement that the federal government lead the efforts in developing processes and capabilities that support the integrity of information technology systems.

In the meantime, there are various technology solutions than can help counter cyber threats to information technology supply chains. Examples of these solutions include:

- Use of PKI and other strong authentication technologies to enable supply chain providers to be sure that they are doing business with the partners they trust, and that information passed between partners is authentic and has not been manipulated.
- Use of detection, prevention, and remediation controls such as a host-based security system (HBSS) to ensure that the systems supporting the supply chain perform as intended and that any attempt to subvert the supply chain through the supporting technology is detected and reported.
- Use of hardware facilities to ensure that the integrity of a system cannot be compromised at the software level, and that advanced capabilities are provided to automatically notify security and operations personnel of potential anomalies that may indicate a security breach.

- Assurance that systems behave in the manner intended, and that controls are in place to ensure, on a continuous basis from the outset, that new commands or corrupted protocol messages are prevented from reaching the application.

In sum, the U.S. needs to find a mix of defense in depth and defense in breadth, the correct balance of technology and protective measures that permit affordable and functional systems that meet reasonable, yet practical, capacity and speed requirements.

3.3 Operational Perspectives on Securing the National Security/ Defense Supply Chain

The Achilles' heel of any supply chain is that it is a highly fragmented process. For DoD, as for most federal agencies and commercial enterprises, it is difficult to ensure that operators, companies, and organizations look beyond their immediate supplier or the next customer in the supply chain.

Do the system integrators research where the individual chips or circuit cards come from? Or do they assume that if these electronic components pass receipt inspection, they are ready for production? When they ship the "black box," do they send it off and track it to the warfighter, or just make sure it gets to the next processor in the supply chain?

Cyber warriors know no borders. While our supply chain business processes are highly fragmented, access to national security supply chains is highly integrated through the convergence of computers and communications. Through the Internet alone, adversaries can find the weakness in fragmented business processes and exploit them. Adversaries can take actions such as:

- Exfiltrating technical data for prime weapons systems like the F-35, which may be used to compromise mission capability in future conflicts.[24]
- Placing "backdoors" into weapons platforms, sensor systems like air-defense radars, and other mission-critical systems, including the electric grid, which can be used to compromise those systems in combat.[25]
- Misdirecting, holding, or delaying shipments.[26]
- Substituting counterfeit parts or equipment.[27]
- Ordering duplicate parts/equipment.

These and other interferences will require resources to track the missteps, and may require reshipment. All cause delay and disruption, inefficiency, and mistrust in the supply system. Deployments may be missed and missions put on hold. Substitution of counterfeit parts can produce a wide range of adverse results, ranging from short-term mission failure to strategic failures caused by a compromise of command and control assets.

DoD efforts in defense of supply chains must be as seamless as its adversaries' means of penetration. To its credit, the Department recognizes this as the nation's greatest supply chain challenge.

Complex new automated maintenance systems employed by the U.S. Air Force are increasing the reliability and endurance of aircraft but can also be targets of cyber attacks that may have crippling effects on military readiness. Photo courtesy of U.S. Air Force.

24 Hon. Loretta Sanchez, CACI-USNI symposium comments.

25 Wallace, op. cit.

26 Hon. Gordon England, CACI-USNI symposium comments.

27 Gilmore, op. cit., citing a 2008 FBI report that found 3,600 counterfeit Cisco chips inside the networks of the Defense Department and power systems of the U.S.

The U.S. Transportation Command is focused on expanding supply chain visibility to better protect goods and services delivered to the warfighter. Seal courtesy of U.S. Transportation Command.

With the designation of the U.S. Transportation Command (TRANSCOM) as the distribution process owner for DoD, delivery processes are on the road to improvement. TRANSCOM, having already experienced no less than 150 cyber attacks, is working to expand supply chain visibility to a true sense-and-respond logistics that reaches back to the suppliers and forward to the warfighter.[28]

However, beyond the distribution process for DoD, U.S. and foreign industrial members of the supply chain remain insulated from each other.[29] Every place there is a seam, there is a vulnerability open to exploitation. The continuing inability to completely integrate the supply chain remains a significant problem. This issue applies not only to new components, equipment, and systems but also to items being returned for repair, whether to a depot or the original equipment manufacturer. Moreover, it is a concern for every industrial base and supply chain partner, both public and private.

How might these risks be mitigated? Significant aspects of a mitigation plan are possible through the application of converged information technology and communications technologies, but employing these technologies must make the situation better; status quo is not an option. What would these technology-based risk-mitigation strategies look like?

28 Wallace, op. cit.
29 Christianson, op. cit.

There are several aspects that might be included. First is early warning.[30] Early warning requires constant monitoring of the environment, the supply chain, the mission status, and the warfighting readiness of the force. Converged, frequent, integrated communication from the private sector all the way to the tactical edge, from the source of supply to the consumer, is vital. Also important is awareness of global events: weather, political, physical conditions, and operational intelligence.[31] Global awareness provides the ability to be predictive and proactive, and to rapidly recover when breaches occur.

No matter how well organizations attempt to prevent security breaches, no systems are ever totally free from vulnerability, and every system can be compromised in some way. This fundamental realization is essential to developing and sustaining the resilient systems essential to mission success.

When breaches occur, what matters is the ability to continue to conduct the mission, or to quickly get back online to provide supplies to the warfighter. Organizations must know when supply chains have been breached, and to what extent. Risk recovery plans must be in place, up-to-date, and well rehearsed. Sufficient alternate inventories, at alternate locations, must exist and be accessible in a timely manner. These will be the measure of logistical success, and probably the combat success of the warfighter.

The paradigm shift to a global marketplace has had staggering implications for securing DoD supply chains.[32] The U.S. no longer builds all, or even most, of the information and communications technology that runs its networks.

Ten years ago, American industry couldn't sell a computer chip to friendly nations without violating export controls. Now U.S.-branded products made in China and other foreign locations are bought and sold routinely. Some sources estimate that as much as 90 percent of the integrated circuits produced in the world are made in China. This means that when a Chinese or other foreign vendor supplies integrated circuits to DoD,

30 Ibid.
31 Ibid.
32 Wallace, op. cit.

they can implant faults or corrupt algorithms in almost any DoD environment, even classified ones. Further, many of our computer manufacturing and Internet companies, Google for example, are a significant part of the Chinese economy. This creates not only an opportunity for corruption but also the potential for divided loyalties. Also factor in that every day, thousands of attacks on U.S. networks emanate from China.

Under these circumstances, DoD, like most enterprises, may be unable to control the products or workforce. The Department is just one of many consumers. It must therefore develop a new cadre of experts.

These must be professionals who can purchase components and products, test them to a satisfactory level, and break away from the mindset that assumes the vast majority of products and services are designed, developed, manufactured, and supported by traditional U.S. manufacturers. In particular, DoD supply chain managers have to be specifically (re-)trained to manage in this globalized environment where the U.S. no longer controls the labor for, or the sources of supply of, hardware and software.

CNCI-11 addresses many of these issues from a converged computers and communications technology supply chain perspective.

Tasked under the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23, the initiative recognizes that significant gaps exist in the U.S. government policy regarding supply chain risk management. In particular, there is no mandate to address risk management in acquisition programs, there are limited risk management tools, and there is a lack of guidance on the use of vendor threat information.

Going forward, the U.S. must determine how to do as good a job of controlling supply chain security as it does controlling the seas with the U.S. Navy and the air and space domains with the U.S. Air Force.[33]

33 Robert Carey, CACI-USNI symposium comments.

4 The Way Forward: A View From the Hill and Beyond

The gravity of the growing threat posed by cyber attacks – especially when measured against the particular vulnerabilities of vital global supply chains – challenges the foundations of our national security and demands a concerted response by the executive and legislative branches. The pervasive and rapidly evolving cyber threats must be countered with forward-thinking, adaptable legislative initiatives implemented with flexible rulemaking.

Although such a concerted response from the legislative and executive branches cannot be expected to anticipate and address every aspect of the cyber threat, it is certainly possible to enhance the efficiency of national efforts. It requires an approach designed to strengthen specific cyber-related legal authorities, clarify the roles and responsibilities of affected executive agencies, and change public perceptions.

4.1 Legislative Branch Initiatives

Recent years have witnessed a wave of legislative initiatives intended to improve cybersecurity. However, attempts to comprehensively address cyber threats have been complicated by a number of factors, including the "uncertainty of the geographic location of the perpetrators of cyber attacks [and] the introduction of new vulnerabilities to the nation's infrastructure from increasingly sophisticated threats."[34] Notwithstanding these formidable obstacles, it is essential to enact legislation that is carefully crafted to advance a comprehensive national strategy capable of adapting to evolving cyber threats.[35]

Strategically, remedial cybersecurity-enhancing legislation should be developed in concert with affected executive agencies, as well as their congressional

34 Catherine A. Theohary and John Rollins, "Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress," Congressional Research Service, September 30, 2009.
35 England, op. cit.

The legislative and executive branches of U.S. government must work together to craft initiatives and implement actions that will be decisive in countering cyber threats. Graphic courtesy of CACI.

oversight committees. The resulting legislation must be sufficiently general to account for emerging technology, while tailored to exploit the particular strengths of the executive agencies that will be charged with its implementation and enforcement. It must also be respectful of the sovereignties of local and state governments, and realistically grounded in the budgetary considerations that will continue to constrain all lawmaking for the foreseeable future.

Additional legislation will be required to create new, key cyber-related positions within the executive branch, and to vest certain existing positions with greater authorities in this area. Although such legislation has been proposed in recent years, no significant initiatives have been passed by both houses. Thus, although legislation that would establish an "office of the National Cybersecurity Advisor" under the cognizance of the President has been introduced, it has not been signed into law. Such an addition to the executive branch, if given sufficient policy-making and budgetary authority, could successfully spearhead meaningful change in the cybersecurity area.[36, 37]

Concomitant with the authority to create such new positions or expand the responsibilities of existing positions should be the ability to offer enhanced compensation to incumbents. A potentially valuable adjunct would be to create a cybersecurity "reserve force" composed of individuals who could leave their private sector jobs to serve temporarily, without jeopardy to their private employment. Along the same lines, the U.S. will benefit from a federal cybersecurity organization with a well-defined charter and attendant authorities analogous – and complementary – to other federal organizations with oversight, direction, and control over a particular area of responsibility, such as the Office of the Director of National Intelligence and the Departments of Defense and Homeland Security.[38]

Such initiatives will require the authorization and appropriation of dedicated funding to accommodate the new organization's start-up and recurring operating costs. Competing budget requirements from other concerned federal agencies, and pressure from state and local authorities for federal assistance, must be balanced to yield resources that are commensurate with the roles and missions of the organization, and the political priority placed on performing them.[39]

Many commentators have noted that the Federal Information Security Management Act (FISMA) is outdated because it has not kept up with the rapid evolution of the Internet and interweaving of converged computer and communications technologies.[40] FISMA has earned a reputation for mandating laborious reporting exercises that do not provide a meaningful picture of an agency's security posture. An agency can get a good FISMA score and still be highly vulnerable. From a governance perspective, when FISMA was enacted it amended the Government Information Security Reform Act, leaving intact the traditional roles of the Department of Commerce's NIST and the National Security Agency, which are not necessarily complementary. In particular, it did not correct the "dichotomy that exists in the treatment of civilian and national security systems."[41]

36 Hon. Jim Langevin, CACI-USNI symposium comments.
37 Theohary and Rollins, op. cit.
38 England, op. cit.
39 England and Sanchez, op. cit.
40 Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002); Langevin, op. cit.; and Langevin, et al., *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, December 2008.
41 *Cyberspace Policy Review*, published by the White House, May 8, 2009.

Further, federal law must be revised to properly incorporate the private sector and foreign allies. Without legislation that supports greater information sharing, as well as military, intelligence, and logistical support to private sector counterparts and allies, U.S. cybersecurity efforts will continue to be challenged.[42]

4.2 Executive Branch Action: Developing and Defining Policy

However carefully crafted, cybersecurity legislation will not be fully effective without concerted, innovative implementation by the executive branch. In this regard, President Obama and his recent predecessors have promulgated executive agency policy initiatives designed to safeguard U.S. national security – including America's supply chains – from cyber threats, including previously mentioned directives like National Security Presidential Directive 54 (NSPD 54) and Homeland Security Presidential Directive 23 (HSPD 23).

Among other things, NSPD 54 and HSPD 23 reportedly authorized efforts that included "safeguarding executive branch information systems by reducing potential vulnerabilities … and anticipating future threats."[43] On May 29, 2009, a little over a year after NSPD 54 and HSPD 23 were formulated, President Obama directed a 60-day policy review of "cybersecurity-related plans, programs and activities." In addition, DoD, the Office of the Director of National Intelligence, and other executive agencies provided policy guidance for their respective organizations.

Notwithstanding these efforts, cybersecurity must continue to rank among the President's highest priorities.[44] This is key to remedying the deficiencies that remain, both in developing an overarching strategic approach to cyber threats, and in prescribing rules to interpret and implement aspects of specific cybersecurity initiatives.

4.2.1 Aligning Agency Roles and Responsibilities

Executive branch policy must better clarify and define agency roles and responsibilities. A particular challenge in chartering any central cybersecurity organization concerns the essential role of converged computer and communications technologies in every domain of endeavor and every federal organization. There will be a corresponding interweaving of charter responsibilities between the cybersecurity agency and every concerned federal agency.

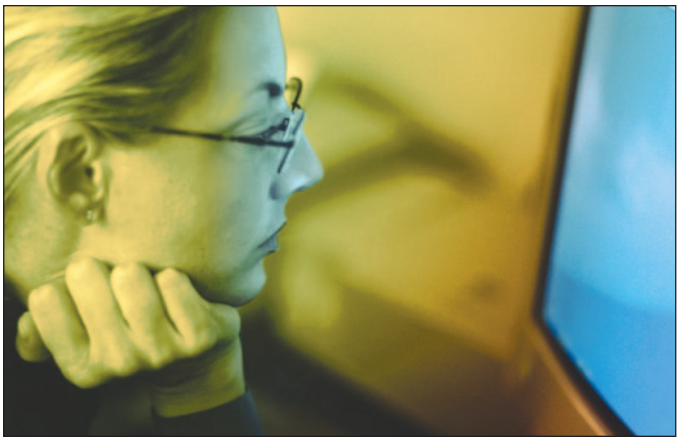
Currently, "agencies have overlapping and uncoordinated responsibilities for cybersecurity activities"[45] under existing executive branch guidance. The CNCI itself faces substantial challenges that cannot be overcome unless roles and responsibilities of "all key CNCI participants … are fully coordinated."[46] Furthermore, greater consideration should be given to performance measures within the CNCI. It is critical to evaluate how well the various government actors are executing on this initiative.[47]

The Departments of Commerce, Defense, and Homeland Security; the Intelligence Community; and other executive branch entities also have various overlapping and potentially competing responsibilities. Presidential policy guidance is required to ensure consistent and complementary implementation of cyber-related authorities that have been prescribed to various federal entities.[48]

4.2.2 Defining Terms

The executive branch must provide policy that precisely and uniformly defines government-wide cybersecurity terminology. Without a common, clearly understood lexicon defining key terms and their connotations, federal agencies will continue to be hampered in forming and carrying out the collaborations necessary to address cyber threats.

42 Langevin, op. cit.
43 Gregory C. Wilhusen and Davi M. D'Agostino, Cover letter to *Government Accountability Office (GAO) Report on Cybersecurity*, GAO-11-338, March 5, 2010.
44 Hon. C.A. Ruppersberger, CACI-USNI symposium comments.
45 Ibid.
46 Ibid.
47 Azmi, private communication.
48 The Department of Commerce's NIST, for example, was directed under the Independence and Security Act of 2007 to oversee various initiatives related to reducing various cyber threats and facilitating an interoperable infrastructure for many agencies. Meanwhile, other departments have similar and seemingly overlapping and/or possibly conflicting mandates.



When is a cyber attack an act of warfare? An ongoing challenge facing governments and lawmakers worldwide is identifying the boundaries between sovereign territory and international "space" in the cyber domain. Graphic courtesy of CACI.

Even the term "cybersecurity" itself has varying connotations and conflicting meanings to different U.S. government departments, including those agencies vested with primary responsibility for U.S. cybersecurity.[49] For example, in DoD, cybersecurity has defensive or offensive military connotations, whereas at other agencies the term refers only to information security.[50]

In order for the executive branch to provide policy direction that binds all government agencies, it must be issued at the Presidential level. Despite recent Presidential attempts to provide additional policy guidance in the cybersecurity area, there is no indication that any of these directives provide the degree of clarity that executive branch entities will require to mount the closely collaborative responses necessary to counter cyber risks.

In addition, a more fully developed legal framework should be adopted for analyzing executive branch cyber-related policies and rulemaking. For example, it is not necessarily clear how the U.S. would legally treat cyber attacks from another nation state under existing policies. If, for example, cyber attacks are, as some predict, the first phase of any attack mounted by U.S. adversaries, what legal recourses would be available to the U.S.?[51]

While attempting to account for the difficulty in attributing responsibility for cyber attacks, executive branch policies also must incorporate more sophisticated legal paradigms establishing the range of potential responses. Although it may be convenient to place cyberspace, like outer space, within the ambit of international law, it is not entirely clear that all cyber attacks necessarily constitute acts of war.[52]

The rules of engagement, including the parameters of a proportionate response and whether there is any such notion as a "just information war" must be addressed.[53, 54] Furthermore, the necessary task of defining boundaries between sovereign territory and international "space" in the cyber domain has proven to be enormously complex. While some have attempted to draw parallels to outer space law and have turned to the United Nations Charter and related treaties and policies for guidance, additional international legal agreements and arrangements will likely need to be promulgated with international partners to ensure a common understanding, implementation, and enforcement.[55]

Greater clarification is also required in existing policy and related legal analysis concerning the definitions of such terms as "cyber criminals" and "cyber terrorists." Without clear definitions, the U.S. will continue to be constrained in acting effectively since the legal rules that apply to each group differ significantly.

4.2.3 The Role of Diplomacy

Diplomatic initiatives, which are the responsibility of the executive branch, will need to complement domestic actions. They should be directed toward addressing the special challenges, threats, and opportunities arising from the cyber domain, which exists beyond physical space and knows no borders.

Initiatives at the international level, such as forming a joint working group with the European Union on common policy supporting cyber protection, intellectual property, and intergovernmental information sharing with regard to cyber threats, are called for. Such an action would create opportunities to advance a smart power perspective.

While there have been initiatives to coordinate international efforts that combat cyber crime and terrorism, such

49 Theohary and Rollins, op. cit.
50 Ibid.
51 Ruppersberger, op. cit.
52 England, op. cit.
53 Langevin, op. cit.
54 Scott Shackleford, "From Nuclear to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, February 20, 2009.
55 Ibid.

The cyber domain crosses all space and borders. International cooperation, achieved through diplomatic initiatives, is necessary for global cybersecurity. Image in public domain.

as the Council of Europe's Convention on Cybercrime, ratified in 2001, significant work remains.[56] Constructs that manage cybersecurity risks must be in place and broadly subscribed to by the international community. To date, there have been no formal international agreements related to the cybersecurity of supply chains.

Implementing agreements between members of the international community is a challenging issue beyond the well-known challenges of diplomacy. The novelty, recent emergence, and lack of agreed-upon cyber terminology add new levels of complexity. The cyber attacks against Estonia in the spring of 2007 illustrate the limits of international understanding of the impact of cybersecurity issues. During the attack, there was difficulty achieving agreement as to whether Article 5 of the North Atlantic Treaty, which requires members of the alliance to render assistance to North Atlantic Treaty Organization (NATO) members that fall under attack, was applicable in the case of the cyber attack against Estonia, a NATO member. Within the cyber domain, there was and is no agreed-upon definition of a hostile act or act of war.

56 Accessed at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm on April 14, 2010.

4.3 A Private-Public Partnership

One of the key aspects of successfully implementing any public policy and a complementary private sector strategy is to ensure proper incentives and disincentives are in place to align private action with societal goals and objectives.

To date, market forces have not favored products with cybersecurity capabilities that make systems secure at the level required for national or economic security.[57] Companies, and by extension broader society, still view cybersecurity as a revenue drain or an add-on, not as an imperative.[58] Consequently, adequately robust cybersecurity products have not benefited from the economies of scale of the global mass market.

The result has been a "market failure" to the extent that the U.S. can't afford the security necessary to survive in a system it created.[59] "We know there are things that we can do that would put these supply chains in better stead in the cyber warfare scenarios," says an officer of the Defense Logistics Agency, which provides supplies and services to America's military forces, "but our customers want us to be cheaper."[60]

Since competition for information technology systems is furious and capability is often considered over security, industry continues to develop insecure systems. Purchasers continue to select "competitively priced" products with insecurity engineered in even while the U.S. becomes increasingly less able to afford them from a security standpoint.[61]

In an environment that demands the enhancement of security in systems and supply chains, it is critical that the U.S. government work with a diversity of market institutions to increasingly make secure products economically desirable. This is essential in stimulating demand for security within the marketplace not only in the U.S. but globally. Coordinated diplomatic activity will also be needed to ensure that more secure products are accepted within the global marketplace.

57 Chabinsky, op. cit.
58 Ridge, op. cit.
59 Chabinsky, op. cit.
60 Edward Case, CACI-USNI symposium comments.
61 Chabinsky, op. cit.

Strategic communications must ensure that every American understands that cyber attacks pose a threat to everything from a single individual to the government at large, to the entire power grid of the nation. Graphic courtesy of CACI.

It is critical to foster innovation and support a global market in secure information technology that will ultimately drive out insecure products. This requires the continued evolutionary development of the private-public partnership that led to those insecure products. Effective communication between the public and private sectors of expectations, goals, objectives, and progress in cybersecurity efforts is needed to ensure that the market is attuned to society's security goals.

The failure of past efforts can be tied to a lack of clear communication of the underlying intent of legislation. For example, the Sarbanes-Oxley Act required corporate top management to certify proper control over financial reporting but did not significantly boost the security of systems, though it could have led to this outcome. Instead, another solution path resulted, one which increased the cost of implementing controls without broadly improving cybersecurity.

Additional policy measures must be adopted to increase joint efforts between the U.S. government and industry partners. Although DoD and other agencies have promoted the sharing of cyber threat information among executive agencies and private sector partners, these initiatives should be broadened to include more private sector participants and greater information sharing.

Government policy should also incorporate measures to ensure that key contractors properly safeguard their systems. DoD has made progress in this area, both by sharing information on threats, vulnerabilities, and best practices with defense industrial base partners, as well as by proposing rules that will raise the standards for information security at companies that store and use DoD information. Efforts like these should be encouraged and built upon, with a clear expectation that it is the responsibility of every organization, public or private, to detect and address lapses or threats to security.[62]

In sum, a judicious balance of actions and incentives will increase market demand for secure, resilient systems in a way that clearly defines and communicates return on investment and supports reasonable costs.

4.4 The Critical Role of Education and Individuals

In the absence of a broadly scaled public education campaign aimed at private citizens, no legislative or executive branch modification of the national cybersecurity apparatus will have its intended effect.

Public officials and private sector leaders must understand and appreciate their roles and responsibilities in preserving cybersecurity and safeguarding the U.S. supply chain. Individual users of government and private information technology systems must be educated regularly on the importance of complying with applicable cybersecurity safeguards. Rank-and-file workers in industries key to converged computer and communications technology, and other U.S. supply chains, must be trained to prevent and deter cyber threats. And every American must perceive the cyber threat in tangible, real terms.

The education of individuals is critical in other ways. Efforts related to establishing enhanced security must recognize and protect the Constitutional right to privacy. Security methods that reduce the level of privacy, or are believed to do so, or impose restrictions that inhibit innovation, or are believed to do so, may not be accepted. Citizens in the U.S. are generally reluctant to support security measures that are perceived as trampling on fundamental freedoms. There seems to be a greater fear and certainty of that than the as-yet unappreciated consequences of a cyber attack that takes down the power grid.

In an open society the right to privacy should be widely recognized, but there is also a recognized need for the assignment and acceptance of responsibility. Unfortunately, the current design and implementation of the Internet and

62 David Wennergren, CACI-USNI symposium comments.

"Cybersecurity is generally thought about in terms of technical challenges. I believe, frankly, the technical side of this is the least challenging. This is an extraordinarily broad, difficult topic that is also a challenge socially, politically, legally, economically, and educationally."

– Former Secretary of the Navy Gordon R. England

cybersecurity systems do not promote this accountability. The Internet provides significant anonymity. Therefore, a critical element in a successful cybersecurity initiative will be a strategic communications initiative that emphasizes that anonymity, which is not the same as privacy, is not a guarantee in the cyber commons.

The cyber threat contends for the public's attention with numerous other issues. There is ample evidence suggesting that the public's perception of the magnitude of the cyber threat does not match the seriousness of the threat. In complementary fashion, the public lacks practical knowledge of cybersecurity best practices or the need for applying them in everyday life.[63]

There is no doubt that the public is challenged not only by the unique nature of the cyber threat but by its ubiquity, its subtlety, and its failure to resemble threats of the past. Key thought leaders have also delivered inconsistent messages. In a recent report, newly appointed White House cyber czar Howard Schmidt was quoted as saying, "There is no cyber war."[64] A week previously, Mike McConnell, former Director of National Intelligence, wrote, "The United States is fighting a cyber war today, and we're losing. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking."[65] In contrast and at about the same time, NATO Director for Policy and Planning Jamie Shea was quoted as having argued that the threat should not be overhyped, insisting that the threat from weapons of mass destruction remains much greater than the dangers of weapons of mass disruption.[66]

63 Langevin, op. cit.
64 Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar,'" Wired.com Threat Level. March 4, 2010. Accessed at http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ on March 9, 2010.
65 Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," *The Washington Post*, February 28, 2010.
66 Julian Hale, "NATO Official: Cyber Attack Systems Proliferating," *Defense News*, March 23, 2010.

5 Findings and Recommendations

The cyber threat is unlike any other threat the U.S. has ever faced.

Other threats, whether symmetric or asymmetric, have employed technologies that directly extend and amplify human physical capabilities. From the spear to the ballistic missile, the tools of war extend the power of the human arm.

Like the human arm, the tools of hard power operate in the familiar domains of land, sea, air, and most recently, space. Never have there been threats of conflicts that take place in a domain that at once instantly connects everyone everywhere and pervades all private and public activities. Never have the technologies that threaten the world directly extended or amplified human cognitive capabilities.

The cyber age has changed everything. Now a computer produced by a compromised supply chain can be just as or more dangerous than a physical weapon. Since the entire supply chain for converged computer and communications technologies can be compromised, our entire information

A critical element in a successful cybersecurity initiative will be communications that emphasize that anonymity is not the same as privacy, and is not a guarantee in the cyber commons. Graphic courtesy of CACI.

technology infrastructure can be thought of as a potential threat, ready without warning to disclose secrets, promote falsehoods, or damage critical property.

Applied to the cyber domain, deterrence tailored to the attribution of cyber attack or manipulation is remarkably hard, owing to the pervasive anonymity of the cyber domain.[67] Creating systems that would offer better attribution is part of the solution, because at present perpetrators in the cyber domain have little risk of being identified and punished for their actions. However, with current technology, it is not easy to associate the cyber attack or manipulation with a source computer. Even if new technologies could better identify a source computer, because of botnets and other forms of cyber manipulation, it is not a given that the owner(s) of the computer took part in the attack. Attribution is far from simple, and unlike nuclear weapons, cyber weapons are ubiquitous.

Traditionally, cybersecurity has focused on purely defensive strategies. Recognizing that the current threat environment consists of constant attack, and that advanced persistent threats from determined adversaries are continuously in play, dictates that other strategies be deployed.

The U.S. government has employed tried and true organizational methods through initiatives like creating the U.S. Cyber Command and recommissioning the 10th Fleet.[68] At the same time it has recognized, in standing up the command, that the sheer interconnectedness of the cyber domain makes it something altogether different from familiar arenas. Since "comprehensive terminology and rules for cyberspace have yet to be developed, even articulating cyberspace threats and identifying options for countering them is extremely difficult."[69]

67 Chabinsky, op. cit.

68 The chief of naval operations (CNO) officially established the U.S. Fleet Cyber Command and recommissioned the U.S. 10th Fleet on Jan. 29, 2010. This was part of the CNO's vision to achieve the integration and innovation necessary for warfighting superiority across the maritime, cyberspace, and information domains. The 10th Fleet was first established in 1941 as the lead for anti-submarine warfare. The global responsibility of today's 10th Fleet is comparable to that of its predecessor, which protected American forces through the use of intelligence and information.

69 Hon. Michael Chertoff, comments from CACI-USNI Asymmetric Threats Symposium Three.

In general, Internet capabilities must be developed to enhance the ability to attribute responsibility for cyber acts to individual networks, computers on the network, and ultimately to a unique human identity. Similarly, additional capabilities must be developed that allow for better control of identified risks and those that have yet to be discovered.

The U.S. must couple defense and prevention with a willingness to actively respond to threats to the cyber supply chain. The government must pursue the development of necessary diplomatic, policy, and legal tools to protect national security and economic interests in a world that the U.S. has been instrumental in shaping. Like the Cold War, where at the outset the U.S. struggled to maintain parity, it needs to invoke and focus the national will and devote the necessary resources to ensuring it achieves and sustains cyber superiority.

To properly support our ability to deter attacks against our cyber and supply chain processes, the U.S. must also devote resources to developing capabilities that will ensure the country has the proper cyber technologies and trained personnel to take their place among the other instruments of national power. In particular, the nation must build the capability to collect and analyze information related to the cyber capabilities of our adversaries, whether criminals, terrorists, or nation states. This is essential to ensuring early warning of impending attacks, notification of attacks in progress, and forensics following an attack.

In addition, as majority owners of the U.S. critical infrastructure, the private sector must be included in the deterrence and defense plans. To support its role,

"Cyber threats can originate from anywhere, at any time, and their credibility is difficult to determine. Unlike traditional warfare, the size of an arsenal is not necessarily a deterrent. The United States is considered to have the most powerful cyber capabilities, but it's still a primary target. Anyone with a network connection is a potential target, making the damage easier to inflict and with greater potential consequences."

– Dr. J.P. (Jack) London

Recognizing that the current threat environment consists of constant attack, the U.S. must devote significant resources to developing cyber technologies and expertise that take their place among all instruments of national power. Photo courtesy of Department of Defense.

the government must develop incentives for assistance as well as mechanisms to protect corporate entities assisting in the national defense. In this connection, it is interesting to note that the notion of the privateer, derived from traditional maritime law, has renewed relevance in cyberspace. The U.S. must also work to minimize the likelihood of unintended consequences.

5.1 Findings

While lacking an established terminology and approach to immediately make sense of the cyber domain and the cyber threat, there are a number of conclusions that can advance national understanding.

Nearly every nation is dependent on the converged computer and communications technologies on which the cyber domain is built, some for virtually every aspect of day-to-day life. At the same time, the wired world has in many, and perhaps most cases, lost the ability to operate in simpler but more secure ways.

For example, traditional seamanship skills such as use of signal flags or lamps to communicate have been abandoned by the fleet, as have navigational skills like dead reckoning based on astronomical observations. If the modern communications and navigation technologies that have replaced the traditional methods were compromised, or rendered ineffective, the fleet's ability to carry out its mission would be, at best, severely compromised. This situation applies across modern society as a whole.[70]

The cyber domain cannot be comprehensively secured. The underlying technologies were conceived of for very different circumstances. There were few computers, computers and general communications had not converged, and physical security for systems was the ultimate and entirely practical guarantee of system security. Nevertheless, the U.S. and nations around the word continue to rely on architectures and systems that are neither secure nor resilient, and are trying to retrofit security on to those systems and architectures.

What can be done will be expensive and time consuming, and will be effective only to an uncertain extent. The economics of cybersecurity inside government, and beyond, are not favorable. The costs of inaction in implementing cyber methods that would protect networks and systems are low, while the costs of implementing effective security measures are high, and must for now compete with other budget priorities.

Cybersecurity and supply chain security are broadly societal problems, not purely governmental problems. There is a diversity of cyber actors, from individuals with criminal intent to nation states, terrorists, and industrial spies. They work singly or in ever-shifting coalitions – and every element of society is a potential target.

The inextricable interconnection of Internet-capable systems brings individuals into close logical proximity to institutional systems, whether corporate, governmental, or non-governmental. Under such circumstances, each individual can be the unwitting dupe of hostile cyber actors.

Furthermore, the revolution in computer and communications technologies has had a leveling effect on society. While symposium participants discussed the need for cybersecurity training of military personnel, the simple truth is that all of us are potential cyber warriors. We each need to be able to rely on all other users to protect the system on which, for good or ill, we all depend.

Policy does not adequately address the cyber threat and has not yet put the U.S. on a path that ensures success. While many elements of this policy are in development,

70 England, op. cit.

the unprecedented scope of the challenge demands an equally unprecedented effort. Tried and true approaches may offer something of value to the U.S. response, but they will be inadequate if they are not reinforced with genuinely innovative approaches to policy. In particular, alliances that emphasize flexibility and agility must be formed among all segments of society, its institutions, and individual members.

5.2 Recommendations

There are a number of specific recommendations that follow from the conclusions that arose from the symposium. These appear below.

A highly reputable public and private consortium should be formed to implement these recommendations. The consortium's goal will be to give the public practical, actionable information that will empower individuals and organizations to understand the significance of the safe use of all Internet-connected devices, as well as each individual's responsibility in protecting all other users.

The campaign must forthrightly and directly address a series of highly sensitive issues, including open society vs. open cyberspace; anonymity vs. privacy and the Constitutional right to privacy; and assignment and acceptance of responsibility.

5.3 Defining Cybersecurity Success

Without a refined evaluation protocol, gauging the nation's success in countering cyber threats will prove at least as elusive as assessing the efficacy of America's response to the more conventional – yet asymmetric – terrorist attack of September 11, 2001.

The absence of a successful large-scale cyber assault against the U.S. only provides a false sense of security.

Similarly, for industry the imperatives must be shared between corporations, government, customers, and the investment community. The role of the investment community is of particular importance because of the

Recommendations

Recommendation 1 – The U.S. needs to aggressively pursue a comprehensive national security policy that ensures the nation is prepared to react to and preempt cyber attacks on systems and critical infrastructure on which American society depends.

Recommendation 2 – Supply chain security must be part of the establishment of an overall cyber intelligence capability that ensures situational awareness and the continuous monitoring of cyber threats. This capability would include collecting, analyzing, evaluating, and disseminating critical cyber intelligence with both national and international partners, as well as developing and implementing appropriate response mechanisms.

Recommendation 3 – The U.S. must develop the ability to build a small number of computer and communication systems that are absolutely certain to be secure. These would be systems built outside of the normal supply chain, from critically secured components sourced only from the U.S. and trusted allies. The cost would be significant, but the effort would ensure the availability of at least a limited number of assured systems architected from hardware and software components that have not been compromised and which can operate with confidence in support of critical activities for key government functions.

Recommendation 4 – The U.S. needs to develop and sustain a strategic communications campaign to provide the public with a realistic appreciation of the cyber threat.

critical role this community plays in assessing how businesses use their capital and operating budgets. If a business's expenditures for all aspects of cybersecurity are judged as investments reducing risk, then the costs of protecting a corporation against cyber threats will be seen as essential to good governance and will enhance shareholder value.

Despite these challenges, certain metrics, if properly defined, can prove useful in assessing legislative and executive branch success in anticipating and countering cyber threats to the national supply chain.

As noted in the *Government Accountability Office (GAO) Report on Cybersecurity*, published March 5, 2010, "Measuring performance allows organizations to track the progress they are making toward their goals."[71] In the cybersecurity arena, benchmarks and milestone reviews can be developed to track implementation progress and gauge the real-world effectiveness of various activities. Cybersecurity initiatives such as those proposed by CSIS could assess effectiveness through periodic testing and such approaches as evaluating the success of "red team" attacks.[72]

Yet, although these measures will provide information relevant to assessing an agency's success in certain areas, any serious effort to determine national success must recognize that cybersecurity is "a process, not a patch."[73] Modifications to the nation's legislative and regulatory cybersecurity apparatus, and the international initiatives necessary to link the global community in common defense, must continue over the long term, as the cyber threat grows and evolves. Evaluating the success of the collective response to global threats will be a process equally as continuous and evolutionary.

71 *GAO Report on Cybersecurity*, March 5, 2010.
72 Ibid.
73 Professor Eugene Spafford, Purdue University, as quoted in James Fallows, "Cyber Warriors," *The Atlantic*, March 2010.

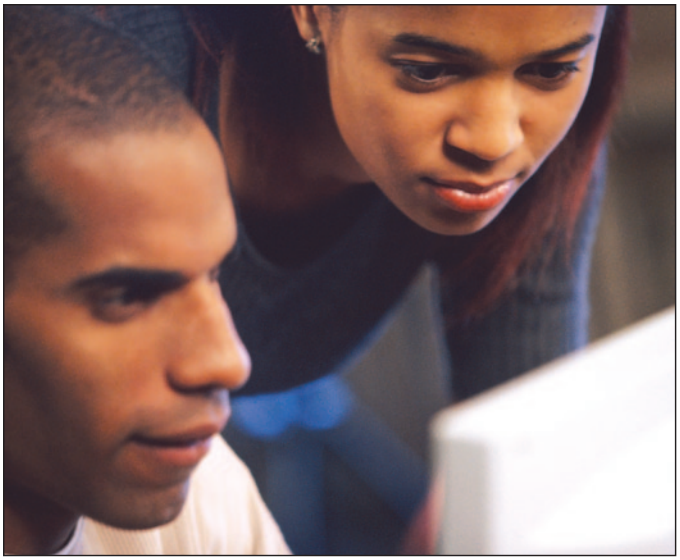
5.4 Conclusion

Cybersecurity is everyone's concern. The increasing dependency on technology has only increased vulnerability to it. That increased interconnectivity has only exacerbated existing security threats around the world.[74]

The findings and recommendations of the symposium on *Cyber Threats to National Security – Countering Challenges to the Global Supply Chain* are intended to advance a national dialogue on defining and examining the nature of cyber attacks, and in particular, in exploring the key area of supply chain security.

The next symposium in the Cyber Threats series is being planned for Spring 2011. As details become final, information will be posted to the Asymmetric Threat website at www.asymmetricthreat.net.

74 Dr. J.P. (Jack) London, USNI-CACI symposium comments.



The cyber domain holds both the source and the solution to cyber threats, and every individual has a role in acting responsibly as a cyber citizen. Graphic courtesy of CACI.

Glossary

Asymmetric threat – A broad and unpredictable spectrum of risks, actions, and operations conducted by state and non–state actors that can potentially undermine national and global security.

Asymmetric warfare – Combat between two or more state or non-state actors whose relative military power, strategies, tactics, resources, and goals differ significantly.

Botnet – A "robot network." Generally regarded as a collection of compromised computers ("robots") operated by remote command and control and running malicious software that the computer's user is unaware of. See also http://www.microsoft.com/protect/terms/botnet.aspx.

Center for Strategic and International Studies (CSIS) – A bipartisan, nonprofit public policy research institution headquartered in Washington, DC. CSIS conducts research and analysis and develops policy initiatives for consideration by decision-makers in the public and private sector. See also http://csis.org.

Comprehensive National Cybersecurity Initiative (CNCI) – Launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 in January 2008, the CNCI consists of a number of mutually reinforcing initiatives designed to help secure the United States in cyberspace: CNCI-11, referenced in the text, is to develop a multi-pronged approach for global supply chain risk management. See also http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Converged Computer and Communications Technologies – A phrase used to emphasize that computer and communications devices today are not distinct, though as recently as 25 years ago this was not the case. At that time, even when computer network data was sent over a communications network, the two were separate. Computers were not used as telephones, and telephones were not used to do "data processing." Neither was used to watch video entertainment. Today, images shot with camera phones distributed over the Internet and viewed on computers are the business processes used by children and jihadists, alike.

Council of Europe Convention on Cybercrime – The first international treaty on crimes committed via the Internet and other computer networks. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. It was ratified in Budapest in 2001 and went into effect on July 1, 2004. See also http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

Cybersecurity – The protection of data and systems in networks that are connected to the Internet by preventing, detecting, and responding to attacks. See also the Department of Homeland Security's U.S. Computer Security Readiness Team website at http://www.us-cert.gov/cas/tips/ST04-001.html.

Cyberspace/Cyber domain – The information environment of the global network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The term was originated by author William Gibson in his 1984 novel *Neuromancer.* See also Joint Publication 1, Doctrine for the Armed Forces of the United States. Accessed at http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

Cyberterrorism – The unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives.

Cyber actors – Any person or entity that communicates or operates in cyberspace. In this white paper, special reference is made to individuals, criminals and criminal enterprises, terrorists, nation states, and corporations. A distinction is also sometimes made between intentional and unintentional cyber actors (the latter motivated by criminal intent but who do not intend to damage national security). See also www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA406949&Location=U2&doc=GetTRDoc.pdf.

Cyber attack – Generally an act that uses computer code to disrupt computer processing or steal data, often by exploiting a software or hardware vulnerability or a weakness in security practices. Results include disrupting the reliability of equipment, the integrity of data, and the confidentiality of communications. As technologies and cyberspace capabilities evolve, the types and nature of cyber attacks are also expected to evolve, so that current definitions should be viewed as foundational rather than final. See also *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress*, updated January 29, 2008. Accessed at http://www.fas.org/sgp/crs/terror/RL32114.pdf.

(U.S.) Cyber Command – A subordinate unified command under U.S. Strategic Command. It was created in June 2009 and achieved initial operational capability in May 2010. Headquartered at Fort Meade, MD, it centralizes command of cyberspace operations with service elements that include the Army Forces Cyber Command; 24th USAF; Fleet Cyber Command; and Marine Forces Cyber Command. See also the Cyber Fact Sheet at http://www.defense.gov/home/features/2010/0410_cybersec.

Cyber criminals – Individuals or groups whose criminal conduct is primarily through or are dependent on operating through cyberspace/cyber domain.

Cyber manipulation – A cyber attack involving an information operation resulting in a compromise of the operation or product delivered through a supply chain. For example, products are delivered to the wrong place, at the wrong time, or not at all, or there is a quality or type problem.

Cyber terrorists – Those who commit acts of cyberterrorism.

Cyber threats – Natural or manmade incidents (intentional or unintentional) that would be detrimental to the cyber domain, or which are dependent on or operate through cyberspace/cyber domain.

DHS Customs Trade Partnership Against Terrorism (C-TPAT) – A voluntary government-business initiative considered the first worldwide supply chain security initiative. Overseen by U.S. Customs and Border Protection, C-TPAT is designed to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. See also http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml and http://www.supplychainsecurity.biz/index.htm.

Doctrine, Organization, Training, Material, Leader Development, Personnel, and Facilities (DOTMLPF) – The standard set of factors to be considered by the military when establishing a new national security capability. See also Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

Federal Information Security Management Act – Title III of the E-Government Act (Public Law 107-347) of 2002. It recognizes the importance of information security to the economic and national security interests of the U.S. and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of that agency, including those provided or managed by another agency, contractor, or other source. See also http://csrc.nist.gov/groups/SMA/fisma/overview.html.

Gilmore Commission – A federally chartered commission formally known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Chaired by former Virginia Governor James S. Gilmore, the commission was formed in 1999 and made five reports to the President and Congress between 1999 and 2003. See also http://www.rand.org/nsrd/terrpanel.

Government Accountability Office (GAO) Report on Cybersecurity – A report by GAO to Congress in which GAO provided requestors with (1) what actions have been taken to develop interagency mechanisms to plan and coordinate Comprehensive National Cybersecurity Initiative (CNCI – see above) activities and (2) what challenges CNCI faces in achieving its objectives related to securing federal information systems. Published March 5, 2010. See also http://www.gao.gov/new.items/d10338.pdf.

Homeland Security Presidential Directive 23 (HSPD 23) – One of two directives issued by President George W. Bush in 2008 (the other being National Security Presidential Directive 54, see below) that formalized a series of continuous efforts to further safeguard federal government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats. See also http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm.

Host-based security system (HBSS) – A system based on an approach to cybersecurity that shifts focus from perimeter security and authentication controls to internal factors. This includes reassessing physical and procedural security practices and considering vulnerability assessments of systems, applications, and interactions with other hosts. See also http://www.windowsecurity.com/articles/Science_Host_Based_Security.html.

ISO 28000 Series – The International Organization for Standardization's specification for security management systems for the supply chain. See also http://www.iso.org/iso/catalogue_detail?csnumber=44641.

National Security Presidential Directive 54 (NSPD 54) – One of two directives issued by President George W. Bush in 2008 (the other being Homeland Security Presidential Directive 23, see above) that formalized a series of continuous efforts to further safeguard federal government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats. See also http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm.

PKI (public key infrastructure) – Enables users of an unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and private cryptographic key pair from a trusted authority. Using the public and private keys, individuals can protect information by encrypting messages and digital signatures and providing for a digital certificate of authenticity. See also http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html.

Supply chain – Starting with unprocessed raw materials and ending with the final customer using the finished goods, the supply chain links many companies together. Also defined as the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain. See also http://cscmp.org/digital/glossary/glossary.asp.

Strategic communication – Focused government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.

(U.S.) Transportation Command – Provides air, land, and sea transportation for the Department of Defense. Located at Scott Air Force Base, IL, the command is composed of three component commands: the Army's Military Surface Deployment and Distribution Command; the Navy's Military Sealift Command; and the Air Force's Air Mobility Command. See also http://www.transcom.mil.

World Customs Organization – An intergovernmental organization exclusively focused on customs matters. It works in areas that include supply chain security and the facilitation of international trade. See also http://www.wcoomd.org/home.htm.

Acknowledgments

Symposium Participants *(alphabetical order)*

Zalmai Azmi
Senior Vice President, Enterprise Technologies and Services Group, CACI International Inc

Robert J. Carey
Chief Information Officer, Department of the Navy

Edward J. Case
Acting Director, Information Operations, Chief Information Officer, Defense Logistics Agency

Steven R. Chabinsky
Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation

Claude V. "Chris" Christianson
Lieutenant General, USA (Ret); Director of the Center for Joint and Strategic Logistics, National Defense University

Paul Cofoni
President and Chief Executive Officer, CACI International Inc

Gordon R. England
Former Deputy Secretary of Defense and former Secretary of the Navy

James S. Gilmore, III
Former Governor of the Commonwealth of Virginia; CACI Board of Directors

Vergle Gipson
Chief of the Analysis Office, National Security Agency/Central Security Service Threats Operation Center

Jim R. Langevin (D-RI)
U.S. House of Representatives

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Dr. Bruce McConnell
Counselor to the National Protection and Programs Directorate Deputy Under Secretary, Department of Homeland Security

Dr. Warren Phillips
Professor Emeritus, University of Maryland; CEO/COB, Advanced Blast Protection; CACI Board of Directors

Tom Ridge
Former Secretary of the Department of Homeland Security

C.A. Dutch Ruppersberger (D-MD)
U.S. House of Representatives

Loretta Sanchez (D-CA)
U.S. House of Representatives

William S. Wallace
General, USA (Ret); CACI Board of Directors

David M. Wennergren
Deputy Assistant Secretary of Defense for Information Management and Technology and DoD Deputy Chief Information Officer

Thomas L. Wilkerson
Major General, USMC (Ret); Chief Executive Officer, USNI

Authors

Hilary Hageman
Vice President, Legal Division, CACI International Inc

Ian Harper
Senior Director, Enterprise Technologies and Services Group, CACI International Inc

Philip M. Sagan, Ph.D.
Executive Director, National Solutions Group, CACI International Inc

Alan Weyman
Vice President, Enterprise Technologies and Services Group, CACI International Inc

Advisors

Zalmai Azmi
Senior Vice President, Enterprise Technologies and Services Group, CACI International Inc

Paul Cofoni
President and Chief Executive Officer, CACI International Inc

Chas Henry
Executive Director of Communications, USNI

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Dr. Warren Phillips
Professor Emeritus, University of Maryland; CEO/COB, Advanced Blast Protection; CACI Board of Directors

Jeff Wright
Senior Vice President, Enterprise Technologies and Services Group, CACI International Inc

Editor

Michael Pino
Publications Principal, CACI International Inc

Reviewer

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

Graphic Design

Chris Impink
Graphic Artist, CACI International Inc

Art Direction

Steve Gibson
Creative Director, CACI International Inc

Stan Poczatek
Senior Designer, CACI International Inc

Publisher and Editor-in-Chief

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Communications Executive

Jody Brown
Executive Vice President, Public Relations, CACI International Inc

Program Managers

Philip M. Sagan, Ph.D.
Executive Director, National Solutions Group, CACI International Inc

Jeff Wright
Senior Vice President, Enterprise Technologies and Services Group, CACI International Inc

Cyber Threats to National Security – Countering Challenges to the Global Supply Chain was held on March 2, 2010 at Fort Myer, Arlington, Virginia.

For more information on the Asymmetric Threat symposia series, visit

http://asymmetricthreat.net

The site includes downloadable white papers from each symposium 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.

July 2010

U.S. Naval Institute
291 Wood Road
Annapolis, Maryland 21402
(410) 268-6110
www.usni.org

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