DEALING WITH TODAY'S ASYMMETRIC THREAT

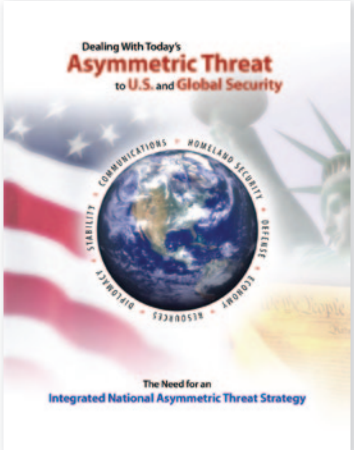
Cyber Threats to National Security

SYMPOSIUM FIVE

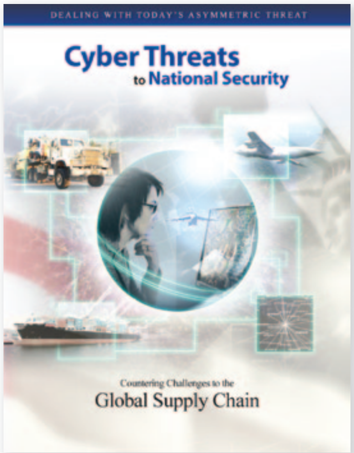
Keeping the Nation's Industrial Base Safe From Cyber Threats

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

Series One



Series Two


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

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

This document is intended only as a summary of the personal remarks made by participants at the March 1, 2011 symposium, “Keeping the Nation’s Industrial Base Safe From Cyber Threats,” held at the Carnegie Institution for Science, Washington, D.C., and co-sponsored by CACI International Inc (CACI), the U.S. Naval Institute (USNI), and the Center for Security Policy (CSP). It is published as a public service. It does not necessarily reflect the views of CACI, USNI, CSP, the U.S. government, or their officers and employees.

The pro bono Asymmetric Threat symposia series was started in 2008 to contribute to the national discourse on the topic of asymmetric threats facing the United States. CACI and the National Defense University sponsored Symposium One in the series, and CACI and USNI sponsored Symposia Two and Three. With Symposium Four, also sponsored by CACI and USNI, a new Asymmetric Threat series was initiated focusing on Cyber Threats. With new sponsor CSP, “Keeping the Nation’s Industrial Base Safe From Cyber Threats” is the fifth symposium in the Asymmetric Threat series and the second in the Cyber Threat series.

September 2011

Contents

Executive Summary

Shortly after entering office, President Obama unequivocally highlighted the safeguarding of cyberspace as a national security priority. Since then, the administration has cited "significant progress in cybersecurity, ensuring that Americans, our businesses, and our government are building better protections against cyber threats."[1] Recently, the administration released its international strategy for cyberspace, a measure the President described as "the first time that our nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues."[2] Though noteworthy, these achievements have not abated the persisting imperative to counter cyber threats systematically, comprehensively, and aggressively. This paper examines that imperative through one critical prism: the industrial base.

The lengthening litany of recent cyber attacks against U.S. infrastructure – apparently of hostile origin – exposes the glaring vulnerabilities of this industrial base. The critical research, production, marketing, and distribution engines of America's economy are at once vitalized by today's dizzying advances in technology and information sharing – and asymmetrically threatened by often anonymous individual and state actors who ride the same currents to infiltrate increasingly edgeless digital networks from within and without.

The situation is further complicated by many Americans' idealized notions of cyberspace, as well as the difficulties in promulgating policies and legislation that clearly assign roles and responsibilities to particular government entities and keep pace with the exponentially evolving cyber medium.

Against this ominous backdrop, the nation's critical infrastructure remains vulnerable to a vast array of cyber attacks, crimes, and other activities inimical to U.S. national security objectives.

Cyber threats to industry emanate from numerous sources. These range from traditional external actors such as rogue states, to highly sophisticated intruders posing an advanced persistent threat, to "inside" sources lurking within the most trusted circles of U.S government, industry and academia. Protecting the industrial base has been further hindered by industrial migration into cloud computing and by the difficulty in ensuring that technological protections in this area are sufficiently dynamic to counter the ever-morphing cyber threat.

The challenge of securing cyberspace and protecting the industrial base against these threats is daunting, but not insurmountable. Success demands a strategy that couples agile, adaptive national security policies with market incentives designed to spur private forging of the technological shields and swords required to defeat a technology-driven enemy.

Any strategy to defeat the cyber threat and protect America's industrial base must be supported by flexible legislation that defines government roles and authorities while balancing national security imperatives with personal privacy, and by U.S.-led international agreements that establish norms and enforce sanctions. If carried out among an aware citizenry by federal officials who recognize private industry's indispensable cybersecurity role, and a savvy, technologically educated workforce, such an approach offers the U.S. the surest path to safeguarding its industrial base within a cyberspace that remains more a bustling social and economic forum and marketplace than a battlefield.

[1] *Fact Sheet: The Administration's Cybersecurity Accomplishments*, May 12, 2011, http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_accomplishments.pdf.
[2] President Barack H. Obama, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

1 Dimensions of the Cyber Threat

The scenarios that one can conjure to describe the scope of today's cyber threat are chilling because they are both sweepingly devastating and eminently plausible. The power blackout that brought life's normal rhythms to a virtual standstill for 55 million people in the United States and Canada on August 14, 2003, was the unintended result of strained power lines and power system weaknesses. Yet this accidental disruption to America's infrastructure demonstrated the relative fragility of America's industrial base and foreshadowed its susceptibility to harm, particularly from intentional actors.[3]

Indeed, in more recent years, cyber attacks of hostile origin have exploited glaring vulnerabilities in America's defense of its digital infrastructure. For example, the intentional and unauthorized release of classified U.S. documents through WikiLeaks and the costly, apparently continuing attacks on Sony's PlayStation network[4] both demonstrate that the cyber threat is real, present, and serious. Moreover, the Sony attacks in particular may reflect the disturbing characteristic of asymmetric warfare that targets citizens rather than governments. Though it is hard to determine whether the attack was intended to damage Sony as a corporate entity, or simply to exasperate America's parents, the hackers' wide reach was on display.[5]

The cyber genie is out of the bottle, and the U.S. must not fall behind in establishing and supporting cyber defense, countermeasures, and offensive capability as instruments of national power and strength.

With all power gone from their homes and offices, New Yorkers filled the streets during the August 2003 blackout. Photo by Eric Skiff.

The cyber genie is out of the bottle, and the U.S. must not fall behind in establishing and supporting cyber defense, countermeasures, and offensive capability as instruments of national power and strength.

The threat emerges from a tsunami of technological advances and information sharing. It is washing over bureaucracies, infrastructures, legislation, and cultures with an ever-rising intensity that leaves governments confounded, frightened, and struggling to keep pace. It is also a threat attended with opportunity. The revolutionary wave of the "Arab Spring," for example, is being nurtured through social media outlets that enable insurgent leaders to rally support. At the same time, autocratic regimes are fighting back with their own cyber measures, prompting the State Department to fund cyber defense training as a counter response.

Although cyberspace can be an arena for positive and stabilizing impulses that sustain a nation's identity, it can also be a battlefield on which threats from outside and within jeopardize a nation's security. In this light, while some nations view their citizens' access to cyberspace as an avenue of healthy communication, others regard such access as a risk. The most enlightened nations clearly see it as both, and struggle to settle on the degree

[3] Dr. J.P. (Jack) London, Symposium Five comments.
[4] Hayley Tsukayama, "Sony hit with attacks in Greece and Japan," *The Washington Post*, May 24, 2011.
[5] PlayStation Network services were down for two and one-half months, affecting more than 100 million customer accounts (the second-largest online data breach in U.S. history), and will cost Sony an estimated $173 million. Mariko Yasu, "Sony to Complete Restoration of Online Services This Week," *Bloomberg News*, http://www.bloomberg.com/news/2011-07-04/sony-to-resume-playstation-network-services-in-japan.html, accessed on July 5, 2011.

of cybersecurity they can afford in terms of resource investment and constrained individual liberty.

Given the struggles of even the most developed countries in controlling relatively concrete problems such as conventional crime and illegal immigration, some view cyberspace as an unleashable force that cannot be regulated without a cyber "kill switch." However, even if control of the cyber world is unachievable, the threats it harbors can be mitigated. There is a way that proactive governments committed to information and technology security can operate effectively within that world to advance their national objectives.

In this context, and with the objective of furthering the dialogue concerning the future of U.S. security in the cyber era, this paper evaluates the cyber threat from one critical perspective: the industrial base, and the overarching strategies and specific measures that should be undertaken to protect it against cyber attacks from outside, and within.

1.1 Vulnerabilities of the Industrial Base

America's industrial base may be defined as the total industrial capacity (including the capacity of repair and maintenance facilities) of the U.S. economy or nation available for use.[6]

The industrial base has, increasingly, become a technology-enabled environment. This means that the machines Americans most depend on – cars, planes, even pacemakers – all will soon have remote diagnostic capabilities. Cyber threats to an industrial base of this kind will therefore not only be aimed at networks. Nor will the cyber threat be only a remote intrusion issue. The standard vectors seen in this area will be supply chain and vendor.

The design, manufacture, delivery, installation, repair, upgrading, and updating of these products give adversaries of the U.S. significant entrance points to U.S. systems. The supply chain provides multiple points for intrusions, and as the technology environment evolves and becomes increasingly wireless, those with malicious (or worse) intent have increasingly proximate access. Not only can hackers, criminals, and states (rogue or otherwise) passively monitor industrial activity, but they can also pose as wireless access points and start drawing in communications that are riding on networks. The result is insiders who no longer have to depend on remote intrusions. In this scenario, trying to develop a strategy to detect and eliminate intrusions would seem an almost insurmountable problem. It is clear that trying to develop a strategy in this area is a "whack-a-mole problem."[7]

Cyber attacks on America's technology-enabled industrial base can strike at multiple points and come from both outsider and insider threats. Graphic courtesy of CACI.

1.1.1 Assurance and Attribution

Protecting America's industrial base from cyber threats is already a national security priority. Cybersecurity is a major component of the National Infrastructure Protection Plan (NIPP) developed by the Department of Homeland Security (DHS) in 2006.[8]

Cybersecurity policies must also carefully balance technology development and risk management. For example, cloud computing is a growing trend, but it requires a higher level of protection to ensure data reliability, availability, and security. Given that it owns some 85 to 90 percent of the

[6] Also see http://www.businessdictionary.com/definition/industrial-base.html.

[7] Steven R. Chabinsky, Symposium Five comments.

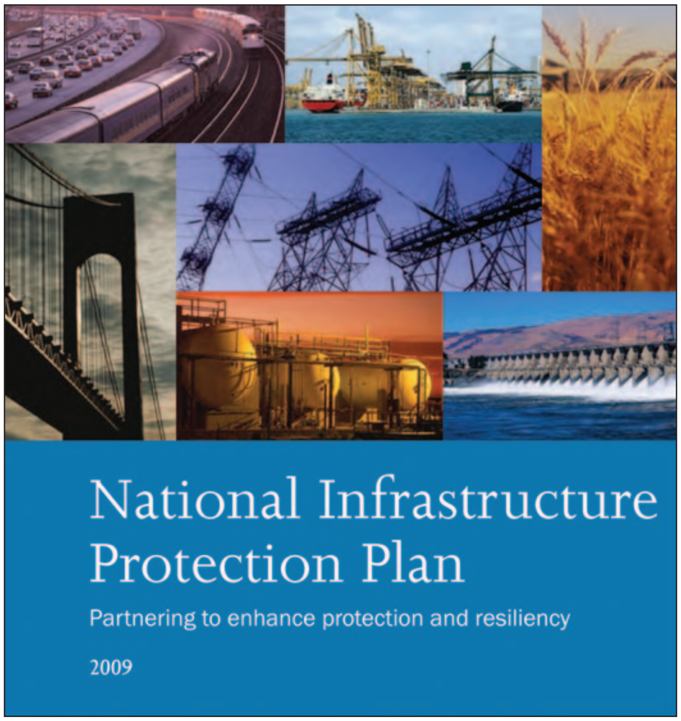
[8] London, op. cit.

nation’s infrastructure, the private sector has placed itself “on the front line of U.S. national security.”[9]

> ***“Cybersecurity efforts must be anchored by dynamic national cybersecurity policy frameworks that direct all government agencies in a coordinated and integrated fashion.”***
>
> *– Dr. J.P. (Jack) London*

Missing in this situation are valid capabilities that relate to assurance and attribution, without which deterrence and threat mitigation are lacking. Assurance is the confidence to know whether data, software, or hardware has been changed. Without it, trust in systems cannot be maintained.

In the initial stages of the technology-enabled environment, when data and software resided on hardware in physical locations, it was much easier for private organizations to detect breaches to their systems. In the present environment of seamless cyber connectivity, in many cases only the government, armed with the latest intelligence and technologies, is equipped to detect penetration. In a virtual environment, such detection is beyond the capability of many, if not most, organizations due to their lack of access to information and technologies that would enable them to better defend themselves. “When an organization does not know it has been infected, it may not be possible for it to eliminate and deter future breaches, let alone identify and have recourse against a perpetrator.”[10]


National Infrastructure Protection Plan
Partnering to enhance protection and resiliency
2009

The National Infrastructure Protection Plan unifies and integrates America’s critical infrastructure protection efforts into a single national program. Image from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Although an organization may try to implement security processes and procedures to protect its systems, such measures are susceptible to penetration. For example, even the most advanced hardware token used to protect sensitive systems from unauthorized access is subject to loss or theft. Merely the theft or loss of one token, therefore, could compromise and otherwise harm an organization’s entire system. “Once a malicious actor is inside the cloud in a trusted role, it becomes very difficult to understand the nature of the intent of the actor so that you can understand the nature of the appropriate response.”[11]

Levels of assurance to be attained are not clearly defined in government either, partially because assurance is difficult to quantify. As a consequence, government institutions are unable to implement policies or technical approaches to achieve assurance against cyber threats. At least for the highest classified levels, government must define the levels of assurance, establish measures and metrics, and develop strategies to achieve them. One option, of course, is to physically isolate these data because “high-end hackers can access anything on current unclassified government architectures.”[12]

The work of the FBI and the Secret Service, in conjunction with the Intelligence Community and U.S. allies, in tracking down transnational organized crime brings a note of optimism to this picture. Unfortunately, the syndicates thus eliminated are but the tip of the iceberg, and the situation will worsen as the Internet evolves and more industrial and governmental systems become virtual.

[9] London, op. cit.

[10] Chabinsky, op. cit.

[11] Richard Gray, Symposium Five comments.

[12] Terry Roberts, Symposium Five comments.

Government and industry must work together as trusted partners to mitigate such risks and continually evolve to meet challenges in threat technologies and the realization of vulnerabilities.

1.1.2 Anonymity and Deterrence

Any strategy for deterring cyber threats to America's industrial base must include deterrence, but the anonymity of the Internet makes it all but impossible to identify the sources of cyber attacks, especially if the attackers have greater-than-average technical knowledge.

The difficulty of understanding, at least on a timely basis, the origins of cyber attacks makes the task of strategizing responses difficult. "In this world of cyber threats, the U.S. effectively does not have the calculus of deterrence normally relied on in other national security situations."[13] If the U.S. cannot determine the identity of the attackers, it cannot target the deterrence. A broader consideration is how to deter other than by following a strategy similar to what was used in the nuclear field – the promise of an overwhelming response that causes the would-be initiator of the attack to withdraw before launching it.

Because of the anonymity of the Internet, tracing the origin of a sophisticated cyberweapon like the Stuxnet computer worm may be nearly impossible. Graphic courtesy of CACI.

The anonymity of the Internet is also a consideration in selecting a response if the identity of the attacker is determined, particularly in the case of a kinetic response.

Moreover, there are downsides to kinetic responses to a cyber attack. First, such a response reveals the responder's cyber technical capability, making it easier for other adversaries to develop cyber defenses. On the other hand, with a cyber response to a computer network attack such as Stuxnet, a responder can recede into the background and maintain a good deal of deniability.

A more significant problem is presented by the ongoing consequences of a kinetic response. A cyber response, proportional or disproportional, enables the responder to remain anonymous and to recede, but with a kinetic response, the responder is no longer anonymous and inevitably is engaged. Iran, for example, has tremendous capability and terrorist proxies deployed around the world. A kinetic fight with Iran is "absolutely guaranteed to involve civilian populations around the world."[14] Therefore, in responding to a cyber threat from an actor like Iran, a cyber response may be preferable.

There are also equally difficult legal challenges. "Until the consequences of stealing over the Internet are no different than robbing a bank, and until the consequences of shutting down a power grid, putting lives at risk, and causing airplanes to crash are the same as killing someone with a gun, cyber crimes will continue."[15] This is why Russian criminals now profit more from cyber crimes than from drugs: It is safer, easier, and can be done from the comforts of home. It can be done without attribution and with less risk. And even if such criminals are caught, the consequences are not as severe.

1.1.3 Public Awareness and Understanding

It is important to educate American society about the potential threats posed by cyberspace. This includes questioning the prevailing view that cyberspace, information technology, and rapid advances in communication are always benign and will invariably transform the world for the better.

[13] Ambassador John R. Bolton, Symposium Five comments.

[14] Frances Townsend, Symposium Five comments.

[15] Gilman Louie, Symposium Five comments.

Consider the so-called Jasmine Revolution in China. Social network messages urged people to come to some 13 locations throughout China and demonstrate for a range of grievances. At almost every location, the demonstrators were outnumbered by the police and the security forces. When demonstrations were announced a second time, some observers wondered whether the social networks were being used to generate the Jasmine Revolution or whether this was an Orwellian example of how communication over the Internet could be used to encourage potential dissidents to come out in the streets so that they could be identified by security forces.

> ***"If you come at these issues with the feeling that only good things come out of cyberspace, it's very hard to get yourself keyed up to worry about cyber threats, whether from abroad or from our own population. But these kinds of discussions are sorely needed."***
>
> *– Ambassador John R. Bolton*

It is certainly true that the Internet and the tools associated with it – especially email and social networks – represent dramatic changes in communication. However, the U.S. as a society must be aware that governments can use these same communication tools in direct opposition to their benign intentions to promote self-expression; that is, to establish uniformity of opinion, much like that described in the dystopias of George Orwell and Aldous Huxley.

It is critical for American policymakers, legislators, and citizens to understand that cyber technology can be an enormous force for good in the U.S. economy and society, but it also is a potential vehicle for destructive forces. These forces can operate well below the level of visual and verbal communication of social networks. They operate through computer codes that have a significant impact because they control the infrastructure.

Americans must understand that all of the technology in the information field and cyberspace communication is just that – technology. Whether technology is benign or malignant depends on who is manipulating it and what their intentions are. Any less clear-headed view of technology diminishes the danger of cyber threats, both external and internal.

1.1.4 Federal Policy and Responsibility

U.S. policies also must keep up with changing technologies. The Executive Branch is only beginning to set national policy and advocate for the necessary legal authorities to counter cyber and cyber-related insider threats.

It is a welcome sign of progress in this area that the White House has recently asked Congress to pass legislation that would codify some of the cybersecurity policies the administration had initially wanted the Executive Branch to authorize.[16] This legislation would also add Internet service providers to the list of critical infrastructure operators that the government oversees and supports.[17]

The Executive Branch must also learn to use legislation, and become an advocate for legislation, that both incentivizes positive behavior and protects the private sector. If the government wants a relationship of trust and confidence, it must be willing to advocate for the protections required by the private sector. For example, under the terrorist surveillance program, on a legal request from the Attorney General of the United States, Internet and communications companies provided data to the government. Those companies were then sued by private individuals and public interest groups for having done so.

Another aspect of this issue is the role of the military versus the Intelligence Community. That is, when is a cyber attack an act of war, and when is it clandestine covert intelligence activity? Put another way, when do cyber attacks constitute crimes? When are they examples of espionage? At what point do they amount to acts of war?

Another problem arises even if we are sure an attack is an act of war. Consider this analogy: Assume a nuclear weapon goes off in an American city. The device was placed in a truck parked in a central location, and the weapon was detonated. There were no missiles, no aerial delivery of any kind, no trajectory to track to see that it came from somewhere like North Korea or Iran, only a nuclear detonation and the tragic consequences that follow.

[16] Aliya Sternstein, "White House agrees to let Congress codify some cybersecurity policies," *NextGov.com,* http://www.nextgov.com/nextgov/ng_20110622_2600.php?oref=topnews, accessed June 23, 2011.

[17] Ibid.

After a careful analysis, American nuclear forensic experts tell the President that based on their evaluation of the radiation and the likely source for the enriched uranium that was used in this device, they are 70 percent confident that it was Iranian in origin. However, there is a 30 percent chance that it came from North Korea. What action should be taken? "Do we respond at 70 percent of the level that we would have had we been 100 percent sure? Do we retaliate against 70 percent of the Iranian targets? Do we attack 30 percent of North Korea's targets, just to be on the safe side?"[18]

Unless the government faces this issue now, the nation will face it in a crisis. There will come a moment when the U.S. must act, and these decisions will be made on the fly. "The Executive Branch will do its best, and everyone who disagrees will criticize the decision."[19]

It is important to remember that when regulations are put in place or legislation is enacted, inevitably, there will be second-, third-, fourth-, and fifth-order consequences that are unanticipated. As true as that is for the Executive Branch, where those consequences are considered and policies and regulations are formed, Congress has even less time and expertise, which means "the downstream consequences to some actions may be worse than the lack of policy."[20]

> ***"Do I ever think that there would be a circumstance where a cyber attack would result in kinetic retaliation? Absolutely. Not because that is the most effective way, not because it is easy or doable in real time to know precisely where the attack is coming from. But because there will be such extraordinary political and public pressure on a President to act and respond."***
>
> *– Frances Townsend*

That is not the best way to make a war/no-war decision. Nevertheless, this crisis is coming. A decision will have to be made. There will be a substantial cyber attack. This is evidenced by the degree of computer network exploitation activity targeting both the defense industry and the Department of Defense (DoD).

There is no excuse for a failure of leadership and accountability now that postpones a decision until then. There is no excuse, but there may be a reason, and that reason is the "tyranny of the in-box."[21] Every day, West Wingers come to their offices with a notion about what they would like to get accomplished in the policy process. Unfortunately, the media are calling. "The phone is ringing and the TV is on, broadcasting events in Egypt, or Tunisia, or Libya, or Bahrain. These events must be dealt with – they cannot be ignored. And so the policy process gets put on hold."[22] Someone must take ownership and address these very difficult issues, regardless of what is going on around the world.

An exercise called Cyber ShockWave made this point very clearly. A multi-administration group walked through a simulated mobile-deployed cyber attack. It was not clear where the attack was coming from, but it created a cascading effect. First, cell towers went down, then lights went out across the Northeast. When it was realized that a mobile-deployed weapon was in use, it became critical for citizens to turn off their cell phones. Every time someone turned on a cell phone, a virus was downloaded and became more pervasive. Unfortunately, in the U.S., the President cannot simply tell the American people to turn off their cell phones.

During the Cyber ShockWave simulation exercise, malicious software planted on cell phones rapidly made its way to cell towers and ultimately crippled a large segment of the U.S. power grid. The exercise also revealed how ill-prepared the U.S. may be for a mobile-deployed cyber attack. Graphic courtesy of CACI.

[18] Bolton, op. cit.
[19] Townsend, op. cit.
[20] Ibid.
[21] Ibid.
[22] Ibid.

A successful U.S. cybersecurity policy must define the "cyber line" that, when crossed by a cyber attack, will result in kinetic retaliation. Photo courtesy of U.S. Air Force.

The question then becomes: Does the President have the legal authority to direct the telecommunications sector to shut the towers down? The answer is probably not, but the President will likely take action nonetheless. He will claim that the nation is under attack and exercise his authority as commander-in-chief to direct certain actions in a national security emergency. Later, arguments will ensue over whether he was right or wrong.

Another question the group confronted was: Where is the capability in the government to respond? It did not reside in the DHS. As the simulated disintegration of U.S. infrastructure continued, it was clear that there were no legal authorities, and the President did not have sufficient legal authorities to respond. Still, it was imperative that he act. The American people demanded that he retaliate. In the end, the group did what every administration always does: It turned to the Secretary of Defense and asked what resources were available to respond to the crisis.

Finally, on the policy front, in addition to not having an international policy or international agreements, the United States has not declared a national cybersecurity policy.

Historically, war escalates in a symmetrical fashion: An enemy kills one of our soldiers, and we kill one of theirs. However, it is difficult to determine symmetry in cyber warfare. What will the U.S. do if a country like North Korea attacks NASDAQ or shuts down the New York Stock Exchange?

The U.S. cannot shut down the North Korean stock exchange – such an entity doesn't exist. Will the U.S. drop a bomb that takes human lives because financial damage cannot be inflicted? Where is the line that other nation states recognize they must not cross or risk retaliation? Where is the policy that defines what that retaliation will comprise? That "cyber line" is blurred because the United States "has not thought enough about it."[23]

Related to the lack of policy is the fact that many of the statutes used to prosecute cyber crime are outdated or ambiguous. Justice Department prosecutors worry that if a case is brought under some of these statutes, there is a possibility that the statute itself will be declared unconstitutional because of its vagueness or inapplicability. Legislation such as the Espionage Act of 1918 was not written with these kinds of communications or offenses in mind.

On the other hand, if the U.S. is not prepared to prosecute, it will never learn whether the statutes are sustainable or what corrections are necessary to give law enforcement at least a last line of defense, one that might deter would-be WikiLeakers. WikiLeaks, of course, is just one example of an attack on America's communications infrastructure and classified databases that is as unsophisticated as an attack can be. Yet it was hugely successful, and only one individual has experienced any consequences.

More and more often, the government does not have the tools available to protect society. The irony is that all of the data actually is flowing freely to private-sector corporations and to other governments. That situation will be expected to increase with cloud computing, making it much more difficult for government to protect society, but making information more easily accessible to private-sector companies and other governments.

[23] Louie, op. cit.

2 Assessing the Cyber and Insider Threat to the Industrial Base

According to the Internet security firm McAfee, more than half the world's critical infrastructure organizations have reported being hit by large-scale cyber attacks or infiltrations.[24] China and Russia are both known to routinely probe American industrial networks to find information and vulnerabilities to use as leverage in any future dispute scenario.

In fact, the private sector, over the next few years, may actually be a "bigger target and more vulnerable"[25] in many respects than some governmental institutions, due in large part to its ubiquity in American society. Moreover, the private sector has operated in conditions of relative security for so long that it is less prepared than the public sector to protect itself against cyber threats.

In securing the U.S. industrial base, it is important to note that cyber threats emerge from a panoply of sources. Radical Islam is one such source, but the Russians, Chinese, and many others are also continually testing America's cyber defenses. Threats also come from non-national actors: terrorist cells, thrill-seeking or malicious hackers, disgruntled employees, and others. Efforts to address cyber threats must clearly define potential threats and develop strategies to deal with them. "When it comes to protecting the industrial base, the industrial sector is looking to government to be able to articulate the threat."[26]

Cyber threats to the industrial base include more than just cyber attacks. They also include cyber espionage and exploitation of system vulnerabilities. Hackers are no longer – if they ever were – just kids huddled over their keyboards in a dorm room or parents' basement. At the same time, the threat of individual cyber criminals pales in comparison to that of nation states. Within a few years, a nation state determined to use cyberspace as a strategic weapon will have the ability to eliminate every sensor, device, vehicle, power switch, and light bulb that has an Internet Protocol (IP) address. For most citizens, the 2003 blackout in the Northeast was an inconvenience, but by 2020, almost every device and system imaginable will be on IP. "This will allow a nation state, rogue or otherwise, to use cyberspace as a strategic, not simply a tactical, weapon."[27]

> ***"Just as the easiest way to rob a bank is to own it, the easiest way to compromise a system is to be inside it."***
>
> *– Steven R. Chabinsky*

The insider threat is also very real. Even if it were possible to eliminate all remote intrusions, the problem would not go away because, as has been said, "just as the easiest way to rob a bank is to own it, the easiest way to compromise a system is to be inside it."[28]

In considering cyber threats to the American industrial base, it is important not to focus so intently on the threat from outside so as to lose sight of the insider threat, which comes from three sources:

- The *Classic Insider* has already been tasked to do damage and seeks a position with a specific organization to carry out that task.
- The *Disgruntled Insider* is a person who joins an organization with the best intentions but later becomes dissatisfied. That dissatisfaction causes this actor to decide to do damage after he or she is in place.
- The *Careless Insider* is probably well-meaning but can create dangerous vulnerabilities. This is the individual who inadvertently introduces malware by carelessly connecting personal storage devices or accessing untrusted sites and files. It can be someone who simply leaves a system on when going to lunch, or who writes down a password and leaves it in the top desk drawer.[29]

Another typology of the insider threat is as follows:

- An insider that acts individually to commit harm.
- An insider who is linked to an outsider.

[24] London, op. cit.
[25] Bolton, op. cit.
[26] Michelle Van Cleave, Symposium Five comments.
[27] Louie, op. cit.
[28] Chabinsky, op. cit.
[29] Stephen Smith, Symposium Five comments.

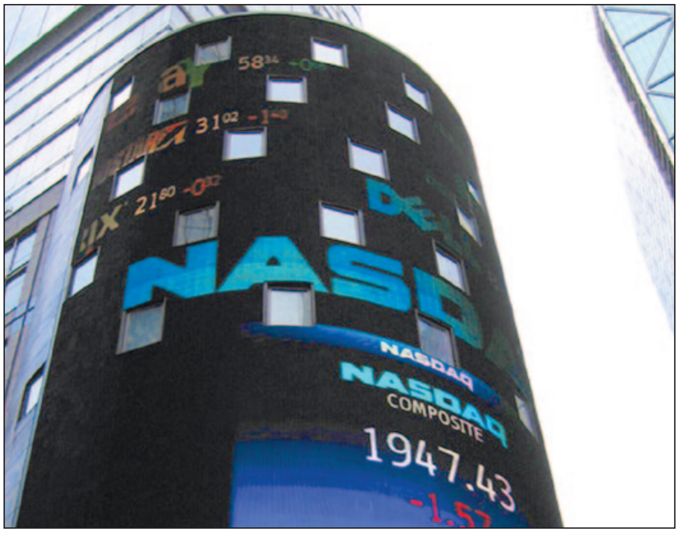
For any comprehensive cybersecurity policy to succeed, it must take into account the real possibility that the most dangerous and hard-to-find adversaries may be those with legitimate access to systems and infrastructure.

2.1 The Realities of the Growing Cyber and Insider Threats

The cyber world is sometimes imagined as one in which everybody gets along and plays by the rules. This is probably best exemplified by the young people of the world who are using Facebook, Twitter, and similar tools to get together and create new structures. Sooner rather than later, we are all going to be talking to each other across borders. As the song says, "We are the world." But do not expect a "kumbaya" world. Rather, we can, and should, anticipate a world in which cyber attacks grow in frequency, gravity, and magnitude.

Consider: The 2008 presidential campaigns of Barack Obama and John McCain suffered cyber attacks. These cyber intrusions were countered relatively easily, but they did force all senior campaign staff to replace their BlackBerries and laptops.[30]

It has not been so easy for DoD. In the first six months of 2009, DoD recorded nearly 44,000 incidents of malicious cyber activity from sources ranging from criminal hackers to foreign governments. Penetrations of Pentagon systems may have been efforts to map out U.S. government networks and learn how to cripple America's command-and-control systems. While the cost in terms of lost data is unknown, remediation for those attacks exceeded $100 million. Cyber espionage alone may have cost the United States up to $200 billion a year.[31]



Cyber attacks like the hacking of the NASDAQ stock exchange in February 2011 may herald an era of cyber warfare on U.S. economic institutions, with results that can range from damaging investor confidence to compromising the U.S. economy on a global scale. Photo by Sean Yu.

On February 6, 2011, it was reported that hackers had accessed the NASDAQ Stock Exchange. In March 2011, Americans learned that the major energy companies were being hit by a series of cyber attacks that started in November of 2009. "Night Dragon" hackers, believed to be Chinese, were able to steal intellectual property and collect data from control systems of global energy and petrochemical companies.[32]

American businesses like Northrop Grumman have also experienced cyber intrusions and disruptions, probably from sites within China. Microsoft had to provide source codes to the Chinese government in order to do business there, and was still subject to cyber attacks. Attacks on Google and its Chinese users were allegedly coordinated at the highest levels of the Chinese government. Chinese cyber spies are known to have penetrated the U.S. power networks to leave potentially disruptive software programs or simply to gain tactical information.[33]

Elsewhere, the Stuxnet computer worm was introduced into the nuclear facilities of Iran, causing centrifuges to spin out of control and actually destroy themselves. At the same time, Stuxnet sent a message to monitoring computers confirming that the reactors were operating normally.

Such incidents underscore the need for caution and readiness on the part of the United States. Indeed, DHS is warning of copycat attacks.[34] The director

[30] Dr. J.P. (Jack) London, "Made in China," *Proceedings*, April 2011.
[31] Ibid.
[32] London, comments, op. cit.
[33] London, "Made in China," op. cit.
[34] Aliya Sternstein, "Cybersecurity center director warns of Stuxnet copycats," *NextGov.com*, http://www.nextgov.com/nextgov/ng_20110526_8466.php?oref=rss?zone=NGtoday.

of the department's National Cybersecurity and Communications Integration Center has expressed concern that malicious cyber actors could use growing public information about the Stuxnet code to reengineer the software to attack broader targets.[35]

Moreover, just as external cyber threats are growing, cyber-related insider threats are also increasing.

On December 4, 2006, U.S. Navy Petty Officer Ariel Weinmann pleaded guilty to desertion, espionage, and other charges. The public record shows that he jumped ship in Connecticut, taking with him an unspecified quantity of classified electronic files.

While he was on duty, Weinmann downloaded detailed national defense information, including such technical manuals as that for the Tomahawk missile. He presented these secret files to representatives of a foreign government at scheduled meetings in Yemen, Vienna, and Mexico City.

Five years later, an Army private was able to take hundreds of thousands of cables and other documents out of a classified network that was not supposed to be downloadable, printable, or manipulable outside of its theoretically secure environment. He accomplished this task by doing nothing more than putting on a set of earphones and listening to music while he downloaded information. "How are sophisticated computer codes useful when a system is so vulnerable to penetration that the very lowest level employee can undertake an activity that has profound consequences?"[36]

WikiLeaks put U.S. sources, methods, diplomats, and forces at risk around the world. Combine this kind of subversion with a sophisticated cyber attack on the U.S. industrial base, and the consequences could be far more profound. Image from WikiLeaks.

WikiLeaks put U.S. sources, methods, diplomats, and forces at risk around the world. Combine this kind of subversion with a sophisticated cyber attack on the U.S. industrial base, and the consequences could be far more profound. The founder of WikiLeaks, Julian Assange, says that his next targets are major American banks and other private-sector entities. His ability to access databases, to make those databases public, or to corrupt, change, or counterfeit them could lead to damage to the U.S. infrastructure that is "all but unimaginable."[37]

There are standing DoD directives that deal clearly and explicitly with the unique regulations that relate to securing classified information systems and digital data. In this light, the case of WikiLeaks becomes a matter of "command responsibility,"[38] and it is, one may assume, being addressed in those channels. This case has also prompted a massive investigation into how all federal agencies protect classified information and how insider threats may be addressed.

On the other hand, the Weinmann case and ensuing damage assessment, which included specific recommendations to rectify this security lapse, brought this looming problem to the attention of national leadership. In 2006, it was thought that "changes would surely be made."[39]

In a DoD action to protect against threats in cleared defense industry organizations, the Defense Security Service (DSS) is investigating the possibility of including contract language with specific details about expected protections to ensure that all bidders understand they must build protection, including insider threat protection, into their systems. It should also be noted that a thorough, competent insider threat program is "defensive, reactive, and offensive,"[40] requiring the support of law enforcement and counterintelligence agencies with investigative and operational authorities.

More often than not, recent espionage cases have involved someone working in industry who has decided to go over to the other side. Clearly, the government must do a better job of helping the industrial base protect itself against insider threats. The DSS, Navy, Army, and Air Force have the authority to work directly with industry and help them from a counterintelligence perspective.

[35] Sternstein, "Cybersecurity center director," op. cit.
[36] Bolton, op. cit.
[37] Ibid
[38] Troy Sullivan, Symposium Five comments.
[39] Van Cleave, op. cit.
[40] Smith, op. cit.

DoD has some 22 organizations that have overlapping counterintelligence (CI) authorities. Each has a responsibility to its parent organizations and to other organizations that do not have their own CI authority. These organizations are responsible for defending against insider threats.

To put "a little intellectual rigor and a little military thinking"[41] into what an insider threat means in DoD, the Secretary of Defense charged the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD/HD&ASA) to create and lead a Defense Department Insider Threat Program. In support of this effort, the Counterintelligence Directorate, Office of the Under Secretary of Defense for Intelligence, and the ASD/HD&ASA developed an approach, based on four pillars,[42] to address the insider threat. The four pillars are as follows:

- *Anti-terrorism Force Protection* focuses on the violent insider extremist in the department.
- *Information Assurance* addresses the person who decides to damage DoD IT systems.
- *Security* concerns the individual who compromises DoD information to unauthorized personnel.
- *Insider Counterintelligence* focuses on the trusted insider who has a link to a foreign intelligence service, an international terrorist organization, or a similar group.

To the extent that these pillars represent four different insider threats, stakeholders are needed from throughout DoD to address them. Although those stakeholders represent different organizations and are primarily interested in different types of threats, to be effective their activities and policies will be integrated. Perhaps most importantly, the Insider Defense Program will review the mitigation activities that each of these stovepipes has been working on to ensure that the mitigation activities of one stovepipe will, in fact, generate information that could benefit the others.

For example, when suspicious activities that are possibly related to an insider threat but do not have a known or suspected link to foreign intelligence services or international terrorist organizations are reported to the Department of Defense counterintelligence specialists, they will forward that information to the appropriate command or law enforcement personnel. This model has been shared with the National Counterintelligence Executive, who is trying to develop an insider threat policy for the federal government.

It is also important to realize that not all efforts should be directed toward defending against the insider who acts alone. The potential for government or private-sector insiders to walk off with large volumes of files is a known threat and there are "known ways of dealing with it."[43]

For every criminal miscreant who individually betrays the trust of the nation, there are hundreds of determined foreign intelligence officers and spies out to undermine America's interests by stealing the proprietary information of the U.S. industrial base and information critical to U.S. economic health and national well-being. In order to stop them, the United States must never forget to continue directing significant energy into learning how these foreign intelligence services accomplish their missions.

2.2 Keeping Pace With Change

To keep up with the pace of technology changes and evolving threats, the business-as-usual approach must be replaced. Business and government must be able to move at the speed of technology in this area, and citizens' freedom of access to cyberspace needs to maintained 24/7.

This is not an area that lends itself to legislation or law enforcement. Fundamentally, America as a whole is relying on legislation and law enforcement systems that were never designed to secure its most sensitive, vital, and critical infrastructures. "The technologists put us in this situation," it has been said, "and the technologists have to get us out."[44] Until this opportunity is recognized, incentivized through the market, and founded on new approaches and technologies, this problem will never be resolved. Continuing to put resources into the current

[41] Sullivan, op. cit.
[42] As presented by Sullivan.
[43] Van Cleave, op. cit.
[44] Chabinsky, op. cit.

architecture is not a viable approach. Similarly, "the interagency approaches that exist today are there to address other challenges and are not effective in this arena."[45]

The DoD Defense Industrial Base Cyber Security Task Force is a major initiative. It is a partnership among some 40 major contractors that receive classified threat information in return for providing information about their loss of DoD information as a result of computer intrusions. The agreement is that if these contractors provide the information, DoD does not penalize them. There is a parallel initiative to add guidance to the Defense Federal Acquisition Regulations about reporting and certain standards that have to be met to do business with the government.

2.2.1 Operational Flexibility

From a policymaking standpoint, the realization of the need to respond at net speed is critical. If nothing else, a "policy lite"[46] must be developed that enables those who have the capability to do so to react immediately, putting them in the position to respond not only appropriately but promptly. Guidelines and rules of engagement must be established that address responses to specific types of cyber attacks. Those who can react most quickly must be identified and put in the position to do so, whether responding to an external or internal threat.

"To survive in the world, many of us learned to mind our P's and Q's. To survive in the cyber world, it's necessary to mind our P's and A's. The A's of cybersecurity are assurance and attribution. On the vulnerability side, the P's are privileges and power."[47]

Users are given privileges that far exceed what they require, along with more powerful hardware and software than they need. These excess privileges and power provide opportunities for mischief and malice. Until these opportunities are recognized and reduced, any vulnerability mitigation strategy is "destined to fail."[48] The WikiLeaks incident is just one example of the damage excess privilege can cause. Employees are reminded to report suspicious behavior because just one person in an organization can make a positive difference. Of course, the other side of the coin is that one person in an organization can also make a negative difference.

It is now possible for one user in a network environment to entirely change the risk posture of an organization in a moment. That is unacceptable. The notion of focusing on privileges and power, therefore, is significant. No progress will be made until the technologists and the economists "start talking to each other"[49] because much of the solution can be market-driven and many of the technologies can be developed. Some of the solutions may bump up against accepted notions of privacy and anonymity. It is therefore probably a good idea to start thinking differently about those systems and services that require privacy and anonymity and the full protections that this country has rightfully grown to uphold.

In the communications arena, whether Twitter or email or VoIP,[50] the government has no oversight and certainly no ownership over the networks. That situation must remain as it is. However, it is also a fact that significant systems and services exist that are responsible for the electric power grid and other critical infrastructure. In these arenas, notions of anonymity and privacy are far outweighed, to the extent that they even exist, by security concerns.

In considering technical solutions for those systems and services where security is more paramount than anonymity, mechanisms must be in place to ensure that transactional data, at least at a certain level, shows provenance. That information may be encrypted. It may be available only with the consent of one of the parties. It may require a court order to obtain – but it must at least ride through communications.

[45] Roberts, op. cit.
[46] Although there is no formal consensus on this commonly used term, broadly speaking "policy lite" may be defined as referring to a less formal U.S. government policy, e.g. less binding than a Presidential Executive Order; or a higher-level but less-detailed and broader policy document that provides flexibility, agility, and adaptability for the government to be as proactive as possible in responding to rapidly evolving challenges such as cyber threats.
[47] Chabinsky, op. cit.
[48] Ibid.
[49] Ibid.
[50] Voice over Internet Protocol. This is a technology that allows users to make voice calls using a broadband Internet connection instead of a conventional phone line. See http://transition.fcc.gov/voip.

2.2.2 Technologies

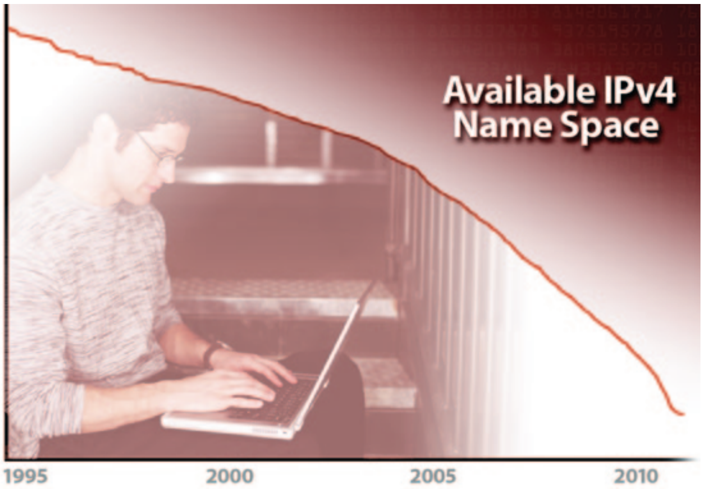
In 1999-2000, the global community underwent a technological transformation: In came the Internet and web-based services, and out went the client server. A major driver of that transformation was concern about Y2K.[51]

Around the world, government and industry leaders and ordinary citizens were worried about the problems that might occur at the stroke of midnight on December 31, 1999. Would absolutely everything quit or collapse? Corporate boards of directors invested billions of dollars to eliminate old software and install new applications that enabled Internet use.

U.S. government organizations initially just patched their way through, then eventually adopted methodologies that industry had started using. This also afforded many organizations the opportunity to take advantage of Y2K to upgrade their infrastructure and increase the reliability of their systems and networks.

A similar transformation, with its own set of challenges, is set to occur again. This time, the transformation will be driven by the move from IPv4, which is running out of name space (the number of addresses to support IP devices), to IPv6.[52] In terms of the name space issue, the Internet will "hit that wall"[53] sometime in 2011.

Some patches will enable IPv4 to survive for a few more years, but sooner or later, the transition to IPv6 will be necessary. At the same time, this is another opportunity to upgrade infrastructure and enhance cybersecurity.



Internet Protocol version 4 (IPv4), which is the foundation for most Internet communications, is running out of space to store Internet address names and will soon be replaced by the next-generation IPv6. However, IPv6 will likely lead to a move to a more virtual environment, which will then be more susceptible to cyber threats. Graphic courtesy of CACI.

2.2.3 Into the Cloud: The End of the Perimeter Defense

The devices running on IPv4 are those that plug into a wall. The devices that will be running on IPv6 are those that run off a battery. The strategies for running on batteries are completely different than the strategies for running off power in the wall.[54]

As any IT professional will note, given the increasing demand and the increasing cost for power and energy, because of power consumption, it is more cost-efficient to replace servers every two years than to allow old servers to continue to run. Because battery power is so critical, by 2014, the current Internet infrastructure will be replaced by a move to the cloud, which is more efficient and allows mobility. In this virtualized environment, many of the trends that are in evidence today will be an order of magnitude faster. However, this new environment also creates new cyber threats.

Anything connected to the Internet is in the "red zone."[55] It cannot be relied upon. Therefore, for critical infrastructure, national security, financial institutions, and the rest of the industrial base, a "green zone" must be created, in which critical components are physically

[51] The problem anticipated when computer applications developed in the 1960s and 70s used six-digit date codes, so that when the date registered 01-01-00, the concern was that the applications would read this date as January 1, 1900 instead of January 1, 2000.

[52] The Internet operates by transferring packets of data across networks as specified by an international communications protocol known as the Internet Protocol (IP). Each data packet contains two numeric addresses that are the packet's origin and destination devices. IPv4 has been the foundation for most Internet communications since 1981. However, the Internet's growth has created a need for more addresses than are possible in IPv4. IPv6 allows for vastly more numerical addresses, but switching from IPv4 to IPv6 may introduce the possibility of increased cyber threats.

[53] Louie, op. cit.

[54] Ibid.

[55] Roberts, op. cit.

or technically isolated. As that green zone is developed, critical infrastructure will operate within it.

The assumption will be that the green zone will be attacked continually. Therefore, its resiliency must be guaranteed. Creating such a zone requires a determination of how to map current networks. The sensor grids that must be in place from the beginning to give common operational pictures of the architecture must also be identified so that, as the zone is attacked, regions of the architecture can be cut off as necessary.

Design and operation of the cloud in this vulnerable environment must be determined, along with the initiatives required to provide warning about low-level germination of new malware activities. It is also vital to recognize that "there will be threat vectors that do not even exist today, making alert capabilities even more critical in order to meet these threats head-on instead of reacting only when they manifest themselves."[56]

Traditionally, cybersecurity strategy has been based on perimeter defense. Whether at Google, Amazon, or the U.S. government, data are put in a physical box, in a physical location. That physical location is secured by armed guards and fences, as well as deep background checks and, in some cases, polygraphs on the people who have access to the location and the data.

> ***"Anybody in the software business will tell you that any hardware hack can hack into any software defense."***
>
> *– Gilman Louie*

That is today. Tomorrow, such data will run in the public cloud. Owners of data will not know where it is, who is running it, who is controlling it, or who is seeing it. What does it mean to have a virtualized system containing secure data that is spread all over the world, running on any computer on demand and vulnerable to hacking?

Because this threat is new, the mathematics and the science behind protecting that data are underdeveloped. Industry and the government are investing billions of dollars in cybersecurity to implement strategies based on current web-based, enterprise-control architectures that will soon be replaced.

The replacement will have no perimeter. For most people, the principal computing device will be a slate or an iPhone tied in virtually to an unknown site. All the security that is currently relied on will be obsolete by 2014.

At that point, when infrastructure and systems are fully controlled by IP, the stakes go up exponentially. "That is when cyber and insider threats will be encountered at a strategic level."[57]

2.2.4 Secure Information Sharing

In formulating security policy to protect against cyber and insider threats, it is worth noting two themes that are at the "front and center of everything that is done across the DoD mission."[58]

- Information should be shared in ways never previously imagined, with up-to-the-minute technologies, across every boundary – among federal agencies; state, local, and tribal governments; nongovernmental organizations; and partners around the world.
- Attacks on government networks, from outsiders and insiders, grow exponentially every day.

Because these two themes are not usually considered to be related, much of the work that both government and private organizations do does not get to the heart of the issue at hand: protecting the industrial base from cyber and insider attacks.

The IT world has shifted dramatically. This is no longer a world of big IT systems that are built to last for years. It is a world of service-oriented architecture. This move from large IT systems to a service-oriented approach introduces a democratization of technology. Organizations no longer hire employees to go off for months to build a solution to a problem. Now, an employee can build a solution at home, overnight.

[56] Roberts, op. cit.

[57] Louie, op. cit.

[58] David M. Wennergren, Symposium Five comments.

Government partnerships with industry have grown exponentially. Most of the research work done internally is now done externally. In these partnerships, any threat to a company that is part of the defense industrial base is a threat to the nation as a whole.

Secure sharing is not a set of isolated problems to solve, but more about two issues that have to be managed effectively to avoid forever falling behind. Considering current security concerns, the answer does not lie in erecting greater obstacles to access or imposing greater isolation on systems. Those actions miss the point, because the U.S. government and industry cannot complete their missions if they cannot reach across boundaries. The need now is to reduce the number of Internet access points in order to monitor information, filter content, and take other steps that promote access, rather than take action that blocks access to an even greater degree.

> ***"If there are thousands of access points to the Internet and none of them is being monitored, the enterprise cannot be secure."***
>
> *– David M. Wennergren*

To be better at information sharing, information security must improve. In fact, "the phrase 'secure information sharing' should replace such terms as 'information security' or 'network defense.' "[59] This may lead to new thinking about the tools that are needed.

With the increasing reliance on cloud computing, data owners will lose control of their information unless rigorous cybersecurity practices and safeguards are in place. Graphic courtesy of CACI.

Both government and industry must better understand technology assets, particularly host-based security systems, and how to determine ways in which these devices and assets are being used for information sharing. In government-speak, this is called "trust in Internet connections … If there are thousands of access points to the Internet and none of them is being monitored, the enterprise cannot be secure."[60]

One possible solution here is the use of secure browsers that let users take nothing out and leave nothing behind. Such answers exist, but the thinking they represent is often not brought into the mainstream, because the focus remains on better intrusion detection and firewalls.

[59] Wennergren, op. cit.

[60] Ibid.

3 Securing the Industrial Base

The value of the Internet to the industrial base is mostly a connected value. Whether data exists in the cloud or on a PC, once the system is unplugged, the data has little value. "Both the public and private sectors now depend on connectivity for efficiency."[61]

It is against this framework that the Homeland Security Council presented its first threat brief. The results were so overwhelming that "the first reaction was to start unplugging systems from the Internet until vulnerabilities could be addressed."[62] However, it is the connected world that must be made robust. The rules of cyberspace that continually increase the predictability of this tool of commerce – rules that allow cyberspace to do what it does and do it ever better and faster – are mostly set by tradition or by the private sector. "The government's role is to ensure that private commerce is not interrupted."[63]

However, within the larger threat context, there is no single government agency, no branch of government, no private company that can by itself counter cyber and insider threats. It requires the full engagement of, and cooperation among, Congress, agency leaders, and industry to bring solutions to this arena. "The way elected representatives and the private industry work together on this issue is critical to the nation's future."[64]

3.1 Private Sector and Citizen Understanding

For more than two decades, technology has allowed individuals and organizations to become much more efficient. For example, companies can hold teleconferences over the Internet, transparently supporting multiple gateways at no incremental cost. Using the Internet to stream video, employ VoIP, and transfer data is, in fact, less expensive than telephone lines and long-distance costs were just a few years ago. Still, some private-sector organizations may be skeptical of the need to invest in cyber protection or may look to the government to address the cyber threat.

U.S. leaders must also consider the role of the public, which is not prepared for a potential disablement of its computers. The public will inevitably be in the middle of the coming cyber war and, therefore, must be included in preparations for this conflict. It is imperative that the American public understand the technical repercussions of potential leaks to U.S. adversaries. "We are motivated, we have incentive, when something touches us closely in our work or at home. And incentives rule the world."[65] Cyber attacks can affect far more than Sony PlayStations.

The worst possible way to address cybersecurity issues is to put up yet another firewall or buy a new PC. Dealing with these threats requires a change in public attitudes and significant private-sector investment. In the long run, the right answers will save money, especially compared to the ineffective (or partially effective) protection provided by the money spent today on stopgap measures.

3.2 Consensus on Privacy vs. National Security

Although protection of privacy is important, it is also important to distinguish from whom privacy is to be protected – the government or the private sector.

Americans' privacy from government is protected by the Constitution, and that protection is one that government agencies must respect. However, privacy under the Constitution has limits. An individual is entitled to a presumption of privacy unless the federal government can demonstrate to a neutral magistrate that there is probable cause he or she is engaged in activities so nefarious that the right to privacy must be infringed. Therefore, the government has the ability to protect its citizens by infringing the privacy of criminals, saboteurs, and the like. Part of the contract of the Constitution is the government's most fundamental obligation to protect its citizenry.

[61] Hon. Darrell Issa, Symposium Five comments.

[62] Townsend, op. cit.

[63] Issa, op. cit.

[64] Paul M. Cofoni, Symposium Five comments.

[65] Major General Thomas L. Wilkerson, Symposium Five comments.

Private citizens, mostly comfortable in today's cyber environment, may not be prepared to support enhanced cybersecurity measures unless the U.S. government ensures they understand their role in safeguarding cyberspace – and know the government is acting in the best interests of their privacy and civil liberties. Photo courtesy of CACI.

The other side of the coin is the degree of privacy that individuals are losing – frequently just giving away – every day to private-sector companies or other governments that do not have similar restrictions. Perhaps paradoxically, critical components of the industrial base are seeking government assistance in securing their systems. It may also be difficult for the younger generation to grasp how much privacy they are giving up and the consequences of doing so, because they are comfortable in the environment.

Mixed use and the notion that everybody is on a device all the time clearly highlight the security-versus-privacy issue. Users on government computers access their private email accounts or, perhaps, their private bank accounts. Those users may feel that they are logging on in a secure, protected environment, but this mixing of official and unofficial use creates a significant problem.

Similarly, there is a problem in determining the division between using an iPhone or a social networking site for personal and business reasons. Dual use makes managing expectations of privacy an enormous challenge.

In a phone-only environment, the expectation of privacy was almost a given. "The world has never faced a telephone system that is 100 percent party line before. Today we have it. The truth is that it's no different than having a house with no curtains, having your telephone line going at all times, and everything you do and say being on camera. Then the question is, 'Is anyone watching? Is anyone listening?' "[66] It is unrealistic to have the same expectation of privacy in the network world of today.

In the discussion of the conflict between the right to privacy and the need for attribution, it is important to maintain the distinction between the web and the Internet. The web should be as anonymous an environment as possible because there is a value to having global free speech. On the Internet – where critical transactions are taking place, where machine-to-machine control is taking place – "attribution is critical if security is to be maintained."[67]

Although it might be beneficial to consider establishing a "policy lite"[68] to set up a framework that allows quick response to net-speed activities, it is not advisable to take privacy and civil liberties lightly. These must be given the highest priority, alongside security, as systems are developed.

In developing cybersecurity control, Congress will be especially concerned about the privacy of individuals because there is no value in protecting the Internet, only to have the Internet take over and "deny the very protections"[69] counted on beforehand.

3.3 Technical and Enforcement Tools

As a start to countering cyber and insider threats, the power of audit and continuous monitoring must be recognized. The U.S. government must move away from a world where certification and accreditation represent a moment in time documented by an immense amount of paperwork. Whether the topic is security clearances (investigate an individual now and again in seven years) or system clearances (check the system now and wait three years to do it again), the point-in-time approach does

[66] Issa, op. cit.
[67] Louie, op. cit.
[68] See Section 2.2.1
[69] Issa, op. cit.

The U.S. government must move away from a world where certification and accreditation represent a moment in time documented by an immense amount of paperwork … Continuous monitoring must be employed to provide alerts to anomalous behavior in real time.

not work. Continuous monitoring must be employed to provide alerts to anomalous behavior in real time.

Automated filters that are part of an audit system may refine the candidate pool of suspect behavior, but at the point at which individuals are identified and cases established and referred for investigative follow-up, appropriate rules must come into play to guide those investigations. That is also the point at which counterintelligence becomes involved because the evaluation of suspect behavior must be done in the context of other information about a specific threat of foreign involvement.

For example, a determination must be made about whether there are known or suspected linkages, whether there is specific information about foreign intelligence targeting particular areas, and whether that intelligence is in the government or the private sector. Additionally, polygraph credibility assessment tools should be used in investigations to give greater insight into potential insider threats. At the same time, as this type of program is instituted, issues of privacy undoubtedly will come increasingly to the fore. They also must be carefully considered.

One of the most significant ongoing initiatives in the Insider Defense Program recently instituted in DoD is to develop a rather ambitious auditing, monitoring, and analysis capability that has become such a high priority since the WikiLeaks incident. The technology is being developed with the idea of auditing and monitoring every DoD computer, regardless of the classification network. As it does so, the Department will address the myriad legal and privacy issues such monitoring involves.

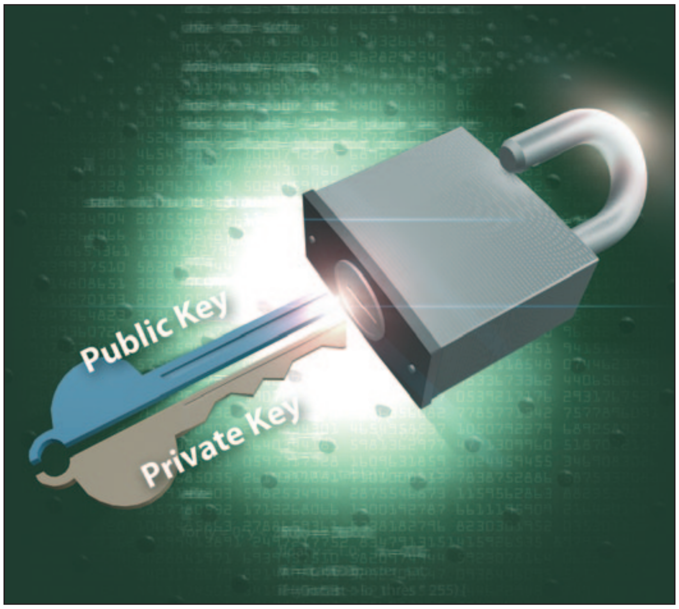
The overall concept is to create a database of keystrokes and downloads, probably at the installation level, and develop a series of triggers that might indicate unusual behavior. Data that indicates suspected anomalous behavior will be reviewed by analysts who will look at the information for potential indicators of criminal activity under one of the four pillars developed by the Counterintelligence Office (Section 2.1) and refer cases to the correct command or the proper investigative organization.

Counterintelligence will be involved until it is determined that there is no "foreign intelligence or international terrorist nexus."[70] When that determination is made, the case will pass to other law enforcement command or other officials.

3.3.1 PKI – the Next Generation of Assurance

Section 1.1.1 of this report discusses problems the U.S. faces in developing capabilities for accurate assurance and attribution. The solution may require increasing focus on public key infrastructure (PKI) and identity authentication.[71]

Generally speaking, PKI establishes encryption algorithms that create a secure method for exchanging information



Public and private key encryption algorithms are part of the evolving solution sets the U.S. will require to provide stronger identity capabilities that can deter – and identify – hostile cyber actors. Graphic courtesy of CACI.

[70] Sullivan, op. cit..
[71] For more on PKI, see the glossary, http://technet.microsoft.com/en-us/library/cc700808.aspx, and http://www.pcmag.com/encyclopedia_term/0,2542,t=PKI&i=49333,00.asp.

over public or private networks. Digital certificates that authenticate the identity of organizations and individuals are used to ensure that messages have not been altered or tampered with. The Defense Advanced Research Projects Agency (DARPA) and the National Security Agency are now looking at PKI and other advanced identity authentication technologies as "part of the next generation of assurance and defense."[72]

At DoD, which has been using PKI certificates on smart cards for years, 3.5 million people are doing cryptographic logon to the network, digitally signing travel claims, encrypting emails when necessary, and using certificates to do secure browsing. They are moving away from a world of user IDs and passwords.

This strong identity capability enables agencies to know who each user is, what device the user is on, where the user is navigating, and what activities the user is performing. The power of identity management is critical in coping with insider threats.

A strong identity capability also provides information on the validity of a member in the user community and the validity of certificates. A user's organization, clearance, and role are known in any given login situation, determining what data the user can access, and what he or she can do with that data. A user with a Secret clearance, for example, does not need to see everything Secret but ought to be able to see the information that the combination of clearance level and specific role allows. To accomplish this, data-tagging is a mundane but necessary task.

The federal government and its industry partners should be able to standardize to combine PKI with personal identity verification (PIV) interoperability cards. The idea is to have one identity card allow its holder to do business with multiple federal agencies rather than a separate identity tied to individual systems or facilities.

A data service is available that allows a driver's license, for example, to be "swiped" and read immediately. The service matches this against terrorist watch lists, the National Crime Information Center (NCIC), and other databases – and does so against real-time data. Services like these need to be made available on a widespread basis so that real-time information can be shared at all installations.

[72] Gray, op. cit.

The Department of Defense is now focused on training a "cyber cadre" of experts who possess the knowledge and skills to advise on and respond to evolving cyber threats. Photo courtesy of U.S. Air Force.

3.4 An Educated Workforce

Skill sets and educational requirements are already changing in the job market. Hiring at the FBI, for example, is increasingly geared toward those with specialized skills. The agency is hiring fewer lawyers and accountants and more people that have technical abilities and language skills. On the intelligence analyst side, the FBI is looking at college graduates with B.S. degrees in electrical engineering and similar disciplines.[73]

Organizations, public or private, concerned with cybersecurity need an "Internet-savvy" workforce. DoD debated the use of social media and social networking services and concluded that it had no choice but to use them. The question was how to use them effectively. The solution to that problem is to have the right kind of monitoring technology, both at the gateway and on individual devices, and to have an Internet-smart workforce. Then social networking tools can be used effectively.

Efforts to educate workers on how to be savvy Internet users are important. One of the potential opportunities organizations have is to attract the young net generation. Members of that generation should be the employees of choice moving forward. Government in particular needs to bring them on board and "unleash their creativity."[74]

[73] Chabinsky, op. cit.
[74] Wennergren, op. cit.

DoD is also focused on building up what it calls the "cyber cadre,"[75] particularly for the Defense Cyber Crime Center. One significant obstacle is that the Department works under the old personnel schemes and compensation programs. One way to overcome this obstacle is to use contractors to perform tasks that might seem to be inherently governmental. The Deputy Secretary is particularly concerned with this and frequently mentions the need for appropriately skilled personnel to build the cyber cadre.

3.5 The Public-Private Partnership

While experts and leaders from government and industry agree that public-private partnerships (P3s) and public-private partnership pilots (P4s) must be part of any effective strategy and program to counter cyber and insider threats, it is clear the U.S. government needs to take the lead on defending the nation's critical infrastructure.

"The private sector owns most of the shoreline, but we still need a navy," said James Lewis, senior fellow at the nonprofit Center for Strategic and International Studies, in testimony before a House Oversight and Government Reform subcommittee hearing.[76] Just as airlines are not asked to defend airspace, businesses cannot be required to protect cyberspace solely on their own. Nor can voluntary regulations adequately resolve the problem. Partnership is the most effective approach.

This partnership could take the form of something like FBI's InfraGard program, which facilitates sharing of actionable intelligence on possible threats among law enforcement, academia, and the public sector.[77] More recently, the National Security Agency has begun a P4 with Internet service providers to deploy new tools in countering cyber attacks against defense contractors.[78] This is a promising sign of progress in public-private collaboration.

Information sharing is key, and though this may be an obvious starting point, it is not without obstacles.

The FBI's InfraGard program, NSA's recent work with Internet service providers, and Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) projects represent promising public/private partnerships that must be part of U.S. cybersecurity policy to protect America's industrial base. Seals courtesy of the respective organizations and programs. Graphic courtesy of CACI.

One difficulty is reaching the appropriate level of sensitivity for sharing information. Another impediment may be the means of transferring information. Because of the "rampant intrusions and data exfiltration"[79] that have occurred in unclassified networks, the focus of one Defense Industrial Base program is on protecting those networks. Participants naturally assumed that they would use their information technology and networks to share information. Unfortunately, in effect they initially proposed to share solutions and cyber threat information on the very networks that had been compromised. Obviously, other sharing mechanisms need to be found, which may be yet another challenge.

This is a time when "the government needs to work with the private sector to define a new paradigm"[80] for a relationship to address cybersecurity. A relationship of trust must be built between the public and private sectors to seriously address the challenges that cyber crime represents to the industrial base. The government cannot do it alone. The government must have the help of the private sector. That is where the intellectual capital to solve this problem resides. A real partnership involves a relationship of trust and confidence.

[75] Gray, op. cit.
[76] Sternstein, "Cybersecurity center director," op. cit.
[77] London comments, op. cit.
[78] Ellen Nakashima, "NSA allies with Internet carriers to thwart cyber attacks against defense firms," *The Washington Post*, June 16, 2011.

[79] Gray, op. cit.
[80] Townsend, op. cit.

Some government agencies complain of insufficient transparency on the part of the private sector with government. However, the government is "not necessarily sufficiently transparent with the private sector, either."[81] Many believe that the information the government has is over-classified and that this over-classification masks a larger problem of insufficient useful information on the part of the government. If the government desires greater sharing from the private sector, these concerns must be addressed.

Issues of competition and market also affect the sharing of information. Unless and until the government can convince a private-sector organization that the government can protect information, both from the organization's competitors and from public disclosure under FOIA or from congressional subpoenas, that organization will not share information.

Nowhere is this more evident than in the financial sector. Banks and credit card companies suffer billions of dollars of loss every year due to cyber crime. Only a small fraction of that is reported to the federal government because of the concern that the public would lose confidence in the financial sector if it understood the extent of the problem.

The difficulties inherent in public-private information sharing can be seen in the financial sector, where banks and credit card companies are often reluctant to reveal cyber attacks on their systems for fear of losing public confidence. For the public-private partnership to succeed, the government must convince these institutions it can both protect their disclosures and help them counter cyber threats. Graphic courtesy of CACI.

To forge a new relationship that will encourage information sharing, work needs to be done on both sides, which will require commitment at senior levels, along with new legal authorities.

Yet another obstacle to information sharing and P4 initiatives (among industry, academia, and government) is the frequent response that activities in this realm are prohibited by current laws. To keep pace with the threat and with technology, the issues that might negatively impact the ability to use P3s and P4s must be identified and resolved. These issues include determining when a public-private voluntary issue affects business relationships, source selections, or contract requirements.

Such legal issues become an obstacle to acting at net speed and responding to cyber threats. The U.S. government must take a certain amount of risk to be able to address these problems because, if nothing else, "U.S. adversaries are not constrained by the same legal frameworks and issues."[82] One recommendation might be to do a low-level pilot with all involved parties and "walk through those decision points"[83] to determine what can – and cannot – be done.

One good example of a successful public-private partnership is the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program.

DIB CS/IA is a family of P4s. The justification for these programs is that the U.S. government has unique insights and information about cyber threats and vulnerabilities and some very sophisticated capabilities to defend against those threats. However, the need exists for new and creative ways to share that information and those capabilities with the private sector, the critical infrastructure. A new model must be put in place that allows this vital sharing.

Put another way, "The soft stuff is the hard stuff."[84] There are many difficulties involved in developing technical approaches for cybersecurity and appropriate responses to intrusions or attacks. To develop these

[81] Townsend, op. cit.

[82] Gray, op. cit.

[83] Roberts, op. cit.

[84] Gray, using a phrase commonly attributed to Dr. Michael Hammer, a founder of the business process reengineering management theory. See also http://www.bizjournals.com/portland/stories/2008/10/20/smallb4.html.

defenses and responses, assurance and attribution must be addressed, the nature of an event must be understood, the source of an attack or intrusion must be identified, and the intent of the actor must be determined. These are all difficult undertakings.

As those in the private sector attempt to confront these issues, it becomes apparent that a new and agile mechanism is needed to keep pace with the threat. Business and government leaders like to think of themselves as being on the cutting edge, being creative and open to new partnerships. However, these same leaders keep falling back on established laws, restrictions, and mindsets. Innovation is confronted with old (perhaps outdated) legal requirements that address competition, unfair preferential advantage, antitrust, and many other issues that inhibit the speed and agility with which public-/private-sector partnerships could be formed.

How should P3s and P4s be structured? One approach is to create a structure that is similar to a critical infrastructure voluntary partnership. In this information-sharing model, all participants come to the table voluntarily. There are no enforcement mechanisms. Another option is a more regulatory approach, one that would require partners to come to the table and that has some enforcement mechanism, such as the DIB CS/IA.

The DIB CS/IA model may work in other environments, but it must be noted that DoD may be in a unique situation. The defense industrial base (DIB) is not only DoD's critical infrastructure sector (for which it is responsible in critical infrastructure schemes), but the DIB is also made up of DoD contractors. U.S. weapons systems are being developed by these contractors, so the background security for the systems on which those technologies are being developed is incredibly important. Separate business relationships must be respected. Creating a model in which a voluntary, friendly, trust-based relationship coexists with a contractual relationship is not an easy task.

Challenges notwithstanding, the program has worked very well. It started as a pilot program with a small group of DIB partners attempting to identify how information could be shared in a secure manner. They were able to make information sharing both secure and much more timely and relevant. Now, they are building the infrastructure to open that information-sharing model to a wider base, not only throughout the DIB but also, to the extent that it makes sense, with such agencies as the Department of Homeland Security (DHS). DHS may then take the lead in spreading the capabilities developed in the DIB CS/IA to other critical infrastructures.

The information being shared in this program is some of the unique cyber threat information held by the DoD and other entities that are very sophisticated in their approaches to cybersecurity. Another set of pilot activities is exploring how the unique information that DoD or government agencies have available can be shared with organizations that depend on commercial services for their cybersecurity.

Much of the work in developing strategies to protect the industrial base has been done in and by DoD and DHS and their contractors, but 85 to 90 percent of the critical infrastructure is in the commercial sector. Therefore, even if the government protects its data and systems, "if cyber criminals can access the intellectual capital of the nation through the government's private-sector partners, everyone is still at risk."[85]

Ideas for sharing information, tips, queuing, and similar issues have been worked for quite some time. Companies that sent representatives to this symposium are working with DoD on how to share that kind of information because doing so is absolutely vital.

From a security perspective, the Defense Security Service (DSS) is the cognitive security and counterintelligence authority in the defense industry. However, DSS works only with Defense-cleared contractors, not the entire industrial base. There have been efforts to rectify this in some way, but just as those efforts were beginning to move with some aggressiveness, they were slowed by budget constraints. The good news, however, is that DSS recognizes that it must do more in this area.

3.6 International Agreements

A frequent suggestion on how to counter cyber and insider threats is to establish international agreements, as has been

[85] Wennergren, op. cit.

done in the arms control arena.[86] Signatories would agree not to engage in cyber warfare. Of course, that may be easier said than done.

Although the cyber infrastructure is a global resource, the management of which requires a new approach to relationships between nations, the risks inherent to such an approach cannot be dismissed. "There are many nations, organizations and individuals who see this as very much a zero sum game and are prepared to take advantage of the sort of globalist approach that we particularly have fostered."[87]

> ***"If one country cannot protect the rest of the world from cyber threats originating on its soil, the rest of the world has an absolute right to do so."***
>
> *– Congressman Darrell Issa (R-CA)*

There are certain classes of behavior that responsible nations can agree should be prohibited. For example, if some actor – a malevolent hacker, a terrorist cell, or a rogue state – shuts down the critical infrastructure of a city or nation, that is unacceptable behavior. "The Chinese have as much interest as the Americans in making sure that the stock exchanges and monetary systems are not corrupted."[88]

One problem with working effectively internationally to counter the cyber threat is the lack of a direct, ongoing interface with cyber staff in European Union countries, which represent more than half of the rest of the developed world. Information from U.S. embassies is funneled to the chief executive. If the President does not initiate action, nothing happens. If the President does initiate action, Congress may question it. Indeed, "Congress is not structured to deal with this problem."[89]

A recommended solution is to engineer a United Nations resolution on cybersecurity and a unified treaty that requires cooperation among nations in the cyber realm.

International agreements on cybersecurity are critical to the global cooperation that is required to defeat cyber threats to the U.S. and all nations. Graphic courtesy of CACI.

This is not like copyright or patent protection, which are win-lose situations. In cybersecurity, with the exception of North Korea, "every nation is a loser"[90] if the environment as a whole cannot be made safe and reliable.

There is an appreciation in the WMD (weapons of mass destruction) community, as just one example, that verification in the biological area is essentially impossible. Nevertheless, any verification argument made in this area would be better than one that could be made for the cyber warfare area.[91]

Another problem in establishing international agreements is that when it comes to international negotiation, friends and allies are not always readily apparent. Consider, for example, how the United States shares intelligence within NATO. It is very restricted, even with close NATO allies. The U.S. simply does not share the most sensitive intelligence with any of its NATO allies and certainly not with all of them. Engaging in complex negotiations with others about cybersecurity poses risks similar to sharing intelligence with allies. Such negotiations may require discussion of sophisticated defensive measures, for example, and may provide information and expose vulnerabilities to those who are not true allies.

[86] President Obama also addressed international cooperation to counter cyber threats in his May 2011 publication, *International Strategy for Cyberspace*, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.
[87] Frank J. Gaffney, Symposium Five comments.
[88] Townsend, op. cit.
[89] Issa, op. cit.
[90] Ibid.
[91] Bolton: "I think you could make an argument, a bad argument, but you could make a better argument in the biological area than you can in cyberspace."

More importantly, and related to the verification question, it could well be that the greatest threats faced in the cyber field are not the ones traceable to, and the result of, obvious actions by nation states. The greatest threats may come from non-state actors who may or may not have some affiliation to any state, organization, or cause. In a world of plausible deniability, that is yet another problem with international agreements.

> ***"There are many nations, organizations, and individuals who see this as very much a zero sum game and are prepared to take advantage of the sort of globalist approach that we particularly have fostered."***
>
> *– Frank J. Gaffney*

Still, as has been noted, in a world of nation states, there are some cyber activities that all might agree are outside the pale, so there may be some role for international agreements. In its deliberations on establishing a national Cyber Command, Congress suggests that, as necessary, international law may be changed to provide the ability to deal, for example, with something like WikiLeaks. Although it is not necessarily a matter that can or should be addressed in an international agreement, laws or policies must also be established to avoid war every time a hacker in China or Albania begins an exploitation of either government or non-government assets.

At the same time, an international agreement may need to be established to shut those hackers down. The tools and the authority to use them must be available, along with an international understanding that "if one country cannot protect the rest of the world from cyber threats originating on its soil, the rest of the world has an absolute right to do so."[92]

Every nation will continue its own espionage activities, and no nation will relinquish the right to use cyber attacks as acts of war when it is attacked or even sufficiently threatened. Certain moves in this arena can be taken off the table, but unless action is taken now, the U.S. and others will always be in the position of throwing up their hands in despair and frustration. Actors will always be attacking from a physical place across America's cyber or global infrastructure, and the U.S. will not be able to touch them. The other alternative, escalating the stakes on both, is equally a recipe for disaster.

The United States has an opportunity to take a role in defining the problem to the rest of the world, including the UN and NATO and countries to which America provides aid, who may themselves be bad actors but want to ensure that the U.S. aid relationship continues. It could be argued before the World Trade Organization that bad behavior in this arena could, in fact, be a legitimate reason for trade sanctions. The U.S. position is that Internet trade is trade. Every country, with the exception of North Korea, is part of this global trade, and that global trade should be enforced and protected. Backing that position is a role for the U.S. government. It is not something the private sector can do.

The private sector cannot convince the world to agree that there must be a strategy, that nation states must work together, and that there must be real sanctions and/or repercussions when actors – individuals, groups, or governments – create a cyber threat or launch a cyber attack. The government is the only entity that can do that.

China, for example, must be made to realize that the world as a whole expects it to stop being part of the problem and start being part of the solution. Not only is the government the only entity that can do this, but it is the entity that *must* do it. "There is no punishment for actors who use cyber tools to mine the research and development efforts of others or who steal information with impunity. This has great impact on America's economic competitiveness and, therefore, on the strength and security of the U.S. industrial base."[93]

The truth is that there are, by far, more cyber attacks for commercial purposes than there are cyber attacks against the government. The government may try to protect its citizens and its assets, including U.S. nuclear weapons, but all of that protection is for naught if the U.S. economy is not viable. And the economy can lose its viability if, every time there is an innovation, it is simultaneously available to every other country. At that point, the driver for innovation is lost.

[92] Issa, op. cit.

[93] Ibid.

4 Recommendations

The cybersecurity threat is an unquestioned national security interest that the U.S. is not prepared or equipped to address. Indeed, as a nation, it has not even done the "intellectual homework"[94] needed to understand the overall nature of the threat. American efforts now are aimed toward protecting the current infrastructure, most of which will be "worthless in the next four years."[95] It is imperative that America systematically expand its thinking about the cyber world and the challenges it will bring in the very near future.

To best protect America's industrial base, all the pieces of the cybersecurity puzzle must fall into place. Graphic courtesy of CACI.

A number of recommendations may be made to advance the national understanding of cyber threats in general and to keep the nation's industrial base safe from cyber and cyber-related insider threats. These appear on the following page.

A public and private partnership is needed to implement these recommendations. No matter how well the federal government is protected from cyber and insider threats, national security is not well served unless America's citizens, commerce, and way of life are likewise protected. Based on both precedents and current and pending legislation, the DHS has the mission to coordinate and lead multi-level and inter-governmental efforts for cybersecurity supporting what this report describes as the industrial base and critical infrastructure.

Cybersecurity and cyber-related insider threats will need to become a major facet of homeland security and homeland defense missions. DHS, with support from the Secretary of Defense and all other federal cabinet heads, has the lead for the National Infrastructure Protection Plan. Inherent in this mission is coordinating across industries and organizations as well as the intelligence, defense, and law enforcement and public safety communities.

These federal efforts must also give the public practical, actionable information that will enable individuals, businesses, and organizations to understand why it is important to use Internet-connected devices and information safely. Each individual must understand how he or she has responsibility in protecting other users. This undertaking requires collective efforts among communities, organizations, and industries to reach the requisite level of risk management and active defense to protect from cyber and insider threats.

Many parts of the nation must come together to ensure a trusted collaboration among the envisioned public-private partnership. The campaign must forthrightly and directly address a series of highly sensitive issues, including open society vs. open cyberspace; security and privacy of commercial and proprietary information; anonymity vs. privacy and the Constitutional right to privacy; liability issues tied to government sharing of threat and risk information; government sharing of threat information with only selected industries and individuals; and assignment and acceptance of responsibility.

[94] Bolton, op. cit.
[95] Louie, op. cit.

Recommendations

Recommendation 1 – Develop a comprehensive and adaptive United States government policy framework that identifies roles, responsibilities, and resources across the government (federal, state, and local) to detect, defend, and preempt cyber threats to the industrial base. Prioritize the development of methodologies and metrics for planning and forecasting resource requirements for cyber defense.

Recommendation 2 – Define the spectrum of cyber threats to the industrial base and potential responses to them. This includes categorizing cyber attacks and which attacks constitute acts of war, as well as cultivating offensive and preemptive capabilities.

Recommendation 3 – Embrace the concept of cyberspace as a military domain, equivalent to the domains of land, air, sea, and outer space, enabling the U.S. government to lawfully target hostile nations and other adversaries. Develop a comprehensive strategic doctrine and rules of engagement governing the offensive use of cyber capabilities by the U.S. Make it clear that the U.S. has ample technical means to act in its national interest and has the capacity to mount a targeted symmetric or asymmetric response in defense.

Recommendation 4 – Strengthen support for National Infrastructure Protection Plan initiatives for integrating critical infrastructure and key resource protection initiatives into a unified national effort. Provide periodic reviews and updates of these initiatives to assure that cybersecurity, supply chain integrity, personnel security, physical security, information security, information assurance, insider threat, and training and education measures and resources keep pace with technology change and evolving threats.

Recommendation 5 – Foster public-private partnerships that provide trusted collaboration to prevent, secure, protect, and mitigate the impact of cyber attacks and cyber-related insider threats. Enact legislation to confer authorities, assign responsibilities, define reporting relationships, and resolve privacy and liability issues to facilitate the degree of information sharing required to support cyber intelligence and insider threat programs.

Recommendation 6 – Encourage the private-sector development of cybersecurity technologies and heightened IT security by offering economic incentives that are realistic and tailored to particular industries.

Recommendation 7 – Make a national commitment to lead world efforts in fostering access to and security within cyberspace – just as the U.S. has done in ensuring freedom of the seas, air, and space – by accelerating the development of legislation, policy, procedures, and authorities. This includes rapidly evolving international and non-governmental partnerships that promote cybersecurity and freedom of access to cyberspace.

4.1 Defining Success

The data needed to gauge the success of security measures taken to counter cyber and insider threats requires not just analysis of the federal government's experience but samplings or measurements of the results of the private sector. This is key even when the private sector is reluctant to report on cyber incidents and the extent of damage caused by these incidents.

Part of the reluctance comes from competitive considerations, but it also comes from a lack of liability legislation needed to foster information exchanges among participants in the public-private partnership. With the private sector "owning" more than 90 percent of the nation's cyber operations, omitting this segment of the nation results in an incomplete measurement of the problem.

There may also be a false sense of security throughout the government and private sector because the U.S. has not been hit by a large-scale cyber attack. Nevertheless, DHS must be adequately resourced and supported by legislation if it is going to lead infrastructure protection efforts, including protection of both the industrial base and the defense industrial base. Among the enabling legislation is the need for a refined evaluation protocol that gauges cybersecurity readiness and vulnerabilities.

As discussed in 2010 in the symposium report on *Cyber Threats to National Security – Countering Challenges to the Global Supply Chain*, without a refined evaluation protocol, gauging the nation's success in countering cyber threats will prove at least as difficult as assessing the efficacy of America's response to the more conventional terrorist attack of September 11, 2001.

The nation needs cyber domain awareness. This requires measurement of cyber infrastructure at all levels of the nation and aggregating and analyzing the information. How to best do this is currently being debated. However, based on the patchwork of federal efforts, antiquated authorities and enabling legislation, and the lack of critical analysis of public-private partnerships, this debate may continue for some time.

Events such as WikiLeaks, Stuxnet, and the Arab Spring have elevated the urgency, complexity, and power of cyber operations and cyber-related insider threats. Whether they result in an acceleration of national efforts to better deal with cyber threats and cyber-related insider threats is yet to be seen. Though there has been an upswing in the tempo of executive and legislative efforts on cyber threats and insider-threat issues, these efforts have yet to provide measurable results.

Each system, each service, each nation state should have an understanding of the level of cyber risk it faces and the level that is acceptable, because the world will never be cyber-risk-free. Each actor will have its own risk calculus. Considering the discrete categories of risk – threat, vulnerability, consequence, and mitigation – at least outlines a path of approach in the cost-benefit analysis of how much risk is acceptable.

Still, determining risk exposure is increasingly difficult, because the proper data points are not available. This makes it difficult to develop a strategy, which presumably is to lower that risk to an acceptable level, recognizing that what is acceptable will be different for different systems, services, and nation states.

In the current situation, neither an acceptable level of risk nor a strategy for sustaining that level has been defined. Most projects in this arena are interim measures, but they have not been considered as a whole to determine whether the degree of risk reduction they offer results in an acceptable level of risk. The real question is not whether such projects will be successful, but what degree of risk remains, and is it survivable? Thus, for all the pilot projects currently underway, in both the private sector and government, one must ask: To what end? What is gained when real-time information-sharing objectives are achieved, other than, perhaps, a short-term tactical benefit?

It is difficult, but necessary, for any U.S. cyber strategy to include clear measures that delineate acceptable levels of risk – and what is gained as a result. Graphic courtesy of CACI.

4.2 Conclusion

Facing the unique national security challenges linked to the nation's, citizens', and economy's use of cyberspace, the United States must do everything in its power to build and implement a comprehensive strategy for dealing with cybersecurity and cyber-related insider threats.

> ***"The development of the Internet and information technology has been an enormously enabling experience for civilization. It has added to trust, communication, productivity, and efficiency … Our task is to preserve this, not to wall things off and make things inefficient because miscreants misuse it."***
>
> *– Former Virginia Governor James S. Gilmore, III*

For the first time in history, cyberspace has become the village square at a global level for knowledge sharing and communications. At the same time, this dependency on technology and interconnectivity has only increased vulnerability to it.

Securing the industrial base is among the challenges the nation faces in building and implementing a comprehensive cybersecurity strategy. Governments at all levels will need to evolve trusted partnerships with industry, communities, and citizens to maximize the positive aspects of cyberspace while mitigating risks. Technology change will not slow down, nor will those intending to use cyberspace to harm the United States become timid in pursuing their objectives through cyber means while governments work out cybersecurity and insider threat issues. As a government and as a nation, the United States must be second to none in implementing and sustaining comprehensive cybersecurity.

Perhaps most important in this discussion of cybersecurity is consideration of the American economy. As long as it is healthy, productive, and growing, the U.S. can surmount the challenges of the 21st century, but that also means that its adversaries can see the advantages of striking at the U.S. through its economy – and "what better way to do so than through a cyber attack?"[96]

There is no partial protection. Nothing takes the place of a proactive and reactive set of defenses. One of the challenges the U.S. faces is to change the dialogue. Addressing cybersecurity in the present is not a question of throwing money at the problem or generating goodwill and cooperation between the public and private sectors. It is about the fact that there are impediments to execution of an effective cybersecurity policy that enables proactive and reactive activity and that gives the American people confidence that their rights are protected.

The U.S. did not establish its nuclear warfare doctrines overnight. It required time to refine its thinking and to apply its efforts to formulating a strategy that enabled it to win the Cold War. A similar larger strategy is needed in the arena of cybersecurity. Clearly, the U.S. cannot protect itself simply by playing defense. "If we resign ourselves to just trying to prevent attacks or mitigating the consequences when we do, we're just inviting more attacks."[97]

The question facing Americans today is whether efforts for integrating the nation's many critical infrastructure and key resource protection initiatives are successful, comprehensive, and adequately resourced and managed to provide long-term frameworks for dealing with a wide range of threats. For now, the answer is no.

The findings and recommendations of the symposium on *Cyber Threats to National Security – Keeping the Nation's Industrial Base Safe From Cyber Threats* are intended to advance a national dialogue on defining and examining the pace of technology change and threats, along with the actions and commitments governments and the public-private partnership can take to mitigate risk, support the economy, and strengthen national security. The industrial base is in some ways the "canary in the mine shaft" for determining if the nation succeeds in implementing a comprehensive strategy for dealing with cyber threats and cyber-related insider threats.

The next symposium in the Cyber Threat series is being planned for Spring 2012. As details become final, information will be posted to the Asymmetric Threat website at asymmetricthreat.net.

[96] The Hon. James Gilmore, Symposium Five comments.

[97] Bolton, op. cit.

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.

Cloud computing – Internet-based computing whereby data, information technology resources, and software applications are stored on the Internet and provided to computers and mobile devices on demand, often through a web browser, rather than running installed software on a personal computer or server. See also http://www.cloudcomputingdefined.com.

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, 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. Actors who engage in these kinds of activities are commonly referred to as cyber terrorists.

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, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

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 ShockWave – A simulated cyber attack on the U.S. that examined how the government would respond to a large-scale cyber crisis. The simulation was hosted by the Bipartisan Policy Center (BPC) on February 16, 2010 in Washington, D.C. and was created by former CIA Director General Michael Hayden and the BPC. The simulation envisioned an attack that disables 20 million smartphones through a malware program planted through a popular smartphone application. The attack escalates, shutting down an electronic energy trading platform and crippling the power grid on the Eastern seaboard. See also http://www.bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats.

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

Defense Advanced Research Projects Agency (DARPA) – A Department of Defense agency whose mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming national security by sponsoring revolutionary, high-payoff research bridging the gap between fundamental discoveries and their military use. See also http://www.darpa.mil/default.aspx.

Defense Industrial Base (DIB) – The Department of Defense, government, and private sector worldwide industrial complex with the capabilities of performing research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, components, or parts to meet military requirements. See also http://www.dhs.gov/files/programs/gc_1189165508550.shtm.

Defense Industrial Base (DIB) Cyber Security Information Assurance (CS/IA) Program – Established by the Department of Defense, the DIB CS/IA program is a collaborative information-sharing partnership between industry and the U.S. government. Under the program, DoD provides threat information, IA best practices, and mentorship to companies to help them better secure their unclassified networks. In return, companies are asked to report network incidents to DoD. See also http://dibnet.dod.mil/staticweb/index.html.

Defense Security Service (DSS) – A Department of Defense agency that provides security support services to the military services, Defense agencies, 23 federal agencies, and approximately 13,000 cleared contractor facilities. See also http://www.dss.mil/index.html.

Hardware token – A physical device that is used to authenticate users who are accessing secured computer systems or networks, such as a private bank account. The simplest hardware tokens generate numbers that are recognized by the system when keyed in. Also called security tokens.

Industrial base – Variously defined, but this report considers it the total industrial capacity (including the capacity of repair and maintenance facilities) of the U.S. economy or nation available for use. See also http://www.businessdictionary.com/definition/industrial-base.html.

Internet Protocol (IP) – The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol (IP) address – A numerical address assigned to each device (e.g., computer, printer) on the Internet. Its most general function is to identify devices that are sending data and devices that are receiving data. Each device on the Internet has at least one IP address that uniquely identifies it from all other Internet devices.

Internet Protocol version 4 (IPv4) and version 6 (IPv6) – IPv4 is the fourth revision in the development of the Internet Protocol and has been the foundation for most Internet communications since 1981. The problem discussed in this report regarding IP versions centers upon the fact that in IPv4, an address consists of 32 bits, which limits the address space to 4,294,967,296 (2^{32}) possible unique addresses. However, because of the enormous growth of the Internet, this address space will soon become depleted. IPv6 was developed in part to solve this problem, as it uses 128 bits for the Internet address, providing the potential for a maximum of 2^{128}, or about 3.403×10^{38} unique addresses.

National Crime Information Center – A computerized system of crime records and data, maintained by the Federal Bureau of Investigation, that can be tapped into by virtually every criminal justice agency nationwide. See also http://www.fbi.gov/about-us/cjis/ncic/ncic.

National Infrastructure Protection Plan (NIPP) – A plan developed by the Department of Homeland Security to provide the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation’s critical infrastructure and key resources into a single national program. See also http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Personal Identity Verification (PIV) – The standard for identification of federal government employees and contractors, as specified in the National Institute of Standards and Technology publication Federal Information Processing Standard Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, and as directed by Homeland Security Presidential Directive – Number 12. The PIV card is an ID card issued by the federal government that contains a computer chip that controls a federal employee's or contractor's access to secured buildings and computer resources. See also http://csrc.nist.gov/groups/SNS/piv/index.html.

Public Key Infrastructure (PKI) – A system of hardware, software, and services that enables users of an unsecured 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.

Stuxnet – A Windows computer worm discovered in July 2010 that targets industrial software and equipment.

Acknowledgments

Symposium Participants *(alphabetical order)*

John R. Bolton
Former United States Permanent Representative to the United Nations

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

Paul M. Cofoni
President and Chief Executive Officer, CACI International Inc

Frank J. Gaffney
President and Chief Executive Officer, Center for Security Policy

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

Richard M. Gray
Associate General Counsel, Office of the Deputy General Counsel for Acquisition and Logistics, Department of Defense

Darrell Issa (R-CA)
Chairman, Committee on House Oversight

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

Gilman Louie
Partner, Alsop Louie Partners; Former Chief Executive Officer, In-Q-Tel

Terry Roberts
Executive Director, Acquisition Support Interagency Acquisition & Cyber, Carnegie Mellon Software Engineering Institute

Stephen Smith
Executive Assistant Director for National Security, Naval Criminal Investigative Service

Troy Sullivan
Director of Counterintelligence, Office of the Under Secretary of Defense for Intelligence

Frances Townsend
Chairman of the Board of Directors, Intelligence and National Security Alliance; Former Homeland Security Advisor to President George W. Bush

Michelle Van Cleave
Former National Counterintelligence Executive

David M. Wennergren
Assistant Deputy Chief Management Officer, Department of Defense

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

Advisors

Louis Andre
Senior Vice President, Business Development, CACI International Inc

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

Christine Brim
Chief Operating Officer, Center for Security Policy

Paul Cofoni
President and Chief Executive Officer, CACI International Inc

Steve Coppinger
Vice President, National Solutions Group, CACI International Inc

Scott Gureck
Executive Director of Communications, USNI

Hilary Hageman
Vice President, Legal Division, CACI International Inc

Jake Jacoby
Executive Vice President, National Solutions Group, CACI International Inc

Ben Lerner
Vice President, Center for Security Policy

Dr. J.P. (Jack) London
Executive Chairman and Chairman of the Board, 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

Dan Porter
Executive Vice President, Enterprise Technologies and Services Group, CACI International Inc

John Quattrocki
Director, National Solutions Group, CACI International Inc

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 Principal, CACI International Inc

Graphic Design

Chris Impink
Graphic Artist, CACI International Inc

Art Direction

Steve Gibson
Creative Director, CACI International Inc

Publisher and Editor-in-Chief

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

Communications Executive

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

Program Manager

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

Event Manager

Janis Albuquerque
Senior Marketing Manager, CACI International Inc

Cyber Threats to National Security – Keeping the Nation's Industrial Base Safe From Cyber Threats was held on March 1, 2011 at the Carnegie Institution for Science, Washington, D.C.

For more information on the Asymmetric Threat symposia series, visit

http://asymmetricthreat.net

ASYMMETRICTHREAT.net
Thought Leadership for Today's U.S. and Global Security Challenges
Search
Visit CACI's website at www.caci.com
CACI
EVER VIGILANT
About This Site
Message from Dr. London
Feedback
National Security Strategy
Enhancing Smart Power
Hard
SMART
Soft
Understanding the Efficacy of Soft Power

Monday, July 11, 2011

This site is a knowledge network to advance the dialogue on national and global security. The goals are to

- Understand the challenges and opportunities
- Present fact-based resources and original research
- Provide a forum for review and discussion of pertinent themes and events

Most Recent Symposium:

Keeping the Nation's Industrial Base Safe from Cyber Threats

Held March 1, 2011

Carnegie Institution for Science
Washington, DC

Conference publication in development now

Knowledge Leaders

Meet the people who are are moving forward the discovery, discussion and analysis of the wide variety of topics related to the asymmetric threat. These are the thought leaders. [more]

CACI Senior VP Zalmai Azmi's Interview with GovInfoSecurity.com
Part 1 - Google Attack: Prelude to More Intrusions
Part 2 - Getting Ready for Cyberwar

Past Symposia

See the agendas, white papers and more details about the past "Dealing with Today's Asymmetric Threat" series of symposia. [more]

Newsroom

CACI, USNI, CSP Announce Symposium on Countering Cyber Challenges to the Industrial Base

Links to recent articles, publications, broadcasts, podcasts and books dealing with topics related to the asymmetric threat. [more]

Global Snapshots

July 2011 - But Are We Safer?

April 2011 - Mind the Gap – What Happens After the Arab Spring?

February 2011 - Lights Out: Securing National Infrastructure from Cyber Threats

Glossary

Learn the language of the asymmetric threat discussion area.

Press Room

Links to articles in the press on the symposia and other associated topics.

The site includes downloadable reports 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.

September 2011

USNI
U.S. NAVAL INSTITUTE

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

CACI
EVER VIGILANT®

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

CENTER FOR SECURITY POLICY

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