IBM Global Business Services

White Paper

Public Sector

Defending Cyberspace: A Framework to Improve Global Performance, Resiliency and Security in the Global Supply Chain

By W. Scott Gould and Peter G. Allor

Acknowledgements

The authors would like to thank the IBM colleagues who contributed valuable insight and support during the process of writing this paper. John Lainhart and Henry Horton provided key guidance to help shape this work. Key comments and feedback were provided by Alan Eisen, John Fairfield, Joi Grieg, Dave Hathaway, Lynn Klar, Kathryn Ignaszewski, Harriet Pearson, and Barbra Symonds. The efforts of Julie M. Anderson and Michelle Cullen helped push this paper through to completion. Suzanne B. Laporte and Leanne Grammenz provided excellent editing and graphic work. Administrative support from Charlyn Isaac was indispensable. Our colleague, Dan Prieto contributed substantially to the discussion of the cyber framework. Finally, this paper would not have been possible without the indefatigable efforts of James Adams, whose insightful contributions laid the foundations of this work.

Table of Contents

Executive Summary

On February 8, 2008, the Director of National Intelligence (DNI) signaled an important change in the nation's approach to protecting U.S. national security in the cyber world when he said: *"The U.S. information infrastructure — including telecommunications and computer networks and systems, and the data that reside on them — is critical to virtually every aspect of modern life…It is no longer sufficient for the U.S. government to discover cyber intrusions in its networks, clean up the damage, and take legal or political steps to deter further intrusions. We must take proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage."* Leaders at the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), among other agencies, are similarly concerned about the extent of the country's interactions in the cyber world and the need for greater security.

The President took initial action to address the cyber threat by submitting to Congress a budget request that allocates $6 billion in 2009 and with the potential to top $30 billion in the next five years to improve cyber security. Exactly who will get to spend the money, and on what, has yet to be decided.[1] Interestingly, the President's move has been welcomed by industry experts, government officials and the privacy lobby as an overdue response to an important problem, but criticized by some as lacking a strategic framework that will ensure effective implementation while guaranteeing civil rights and civil liberties. [2]

The purpose of this paper is to provide:
1) an overview of threats to our cyber infrastructure, 2) a new framework for cyber that is linked to a more secure, resilient and efficient global supply chain, and 3) an analysis of strategic elements of the framework.

Successfully managing the cyber security challenge requires new standards and initiatives, as well as effective governance to ensure compliance. There must be a more robust defense of U.S. cyber interests, while upholding societal values of privacy, confidentiality and civil liberties. Specific components of this new framework include:

- **Leadership.** Meeting the cyber challenge in the U.S. and globally by providing leadership for both the public and private sectors.
- **Governance.** Enforcing across all sectors existing security standards to ensure compliance by network stakeholders as well as software and hardware manufacturers.
- **Civil Liberties and Privacy.** Invoking a transparent process that effectively addresses and ensures civil rights, liberties and privacy concerns.
- **Deterrence.** Establishing a deterrent strategy that will communicate our nation's willingness to respond through a series of escalatory steps against a cyber attacker.
- **Cyber Security Treaty.** Negotiating a Cyber Security Treaty to set standards and impose tough sanctions on any country that fails to comply with clear boundaries of international behavior in cyberspace.
- **Balanced Defense and Offense.** Employing defensive and offensive tactics as part of a credible deterrence strategy.

The success of the new framework will depend on addressing the following considerations:

- **Legal Liability.** A process of legal indemnity may be required for companies damaged by or inadvertently involved in cyber attacks. In addition, a new legal framework for the cyber environment to resolve confusion and conflict in the U.S. and abroad is essential.
- **Law Enforcement.** To police cyberspace effectively, a confidentiality guarantee must be established to encourage the private sector to share information with the government. Checks and balances must be put in place to ensure privacy.
- **Human Capital.** A national campaign of education and training for a cyber security workforce must be developed to mitigate the risks and costs of cyber attacks and to empower front line workers to act on their own initiative when required.

This new framework will bring together government and business in the United States to create a better defended cyberspace, while setting new standards for international behavior that will make the world a safer place.

Cyber Defined

At its simplest, 'cyber' is a word used to define a process or an action that existed in the terrestrial world and that now has a counterpart in the electronic arena.[3]

In this vast, virtual world, millions of people communicate, conduct business, play and interact in ways that were unimaginable just a decade ago. All these activities have associated with them actions that send bits and bytes circling the world. Those actions and reactions provide opportunities for criminals, governments, terrorists and those seeking adventure to interrupt the smooth flow of information and to steal data vital to commerce or national security and attack the systems and networks on which that information resides.

Within the government, the definition of cyberspace remains unclear. The President's National Strategy to Secure Cyberspace never actually defines cyberspace or cyber warfare. To the Department of Defense (DoD), cyberspace is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure."[4]

DoD describes a Computer Network Attack (CNA) as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[5] Computer Network Defense (CND) is defined as "actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks."[6]

To defend against attackers, a defense network has to be established that involves detection of the attacks, the identification of the attacker, the mobilization of defenses and the possible retaliation against the attacker through offensive operations. However, there is no single defense network, no Maginot Line. There is simply the accumulation of defensive measures and systems surrounding individual networks, individual organizations and nodes. And the defenses for each particular node or area are at the discretion of each agency and administered by the people who own and manage those nodes and areas.

The very speed at which the cyber world has developed, combined with the proliferation of users, has led to a free-form and anarchic structure in the virtual world. This web of relationships is similar to the anarchic market structures that existed in global economies as the industrial revolution took hold in the late 18th and early 19th centuries. Today, security in the cyber world is composed of a multitude of individual decisions that largely fail to address the common good. The national system lacks some elements required to address the cumulative need for security such as better coordination, transparency and standards. During the industrial revolution, labor laws, international trading agreements and safety regulations helped to produce order and address risks. Today, that order has yet to appear in cyberspace.

The Public and Private Sector Perspectives

For the government, Information Warfare (IW) is any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.[7] From the private sector's perspective, such actions damage legitimate commercial activity and put a company at a disadvantage in the marketplace. While these two perspectives are different, they are closely related given that every government requires the expertise of the private sector to operate effectively and the private sector, to some extent, needs the information that government may have in order to address potential vulnerabilities or current attacks. And of course, both the public and private sectors rely on the same information technology, especially the World Wide Web, for survival and prosperity. This takes on renewed importance as many government agencies seek to outsource or privatize activities.

However, there remains a largely Cold War paradigm where decisions are made by and for government and those decisions will be of benefit to the population at large in whose name the government acts. Previously, the government was the protector, and the citizens expected to be protected. But, since 9/11, the paradigm has changed dramatically because criminals, terrorists, and some nation states see the entire national infrastructure and not just the government and the armed forces, as legitimate targets. Effective defense is now a matter of shared responsibility between the public and private sectors, including adequate sharing of information between affinity groups and across sectors.

During the Cold War, the intelligence community provided "indications and warnings" of imminent attack. Today, those same indications and warnings are even more important in the cyber realm except that their purpose and content is different. There should exist intimate relationships both within the private sector and between communities of interests in the public and private sectors where real information can be exchanged and where there are mutual incentives to share data. Between some affinity groups, this information might be very granular, and between others it might be appropriate only to share metadata. Exactly where the boundaries should lie and where common interests exist is an open conversation that has yet to happen.

Information Operations (IO) are a concern in every boardroom in every business in the United States. Just how resilient those businesses are to cyber attacks will directly affect the government's ability to respond to a crisis whether through diplomatic means, cyber means or armed conflict.

Security policy can be implemented effectively when security standards are adopted at an architectural level, i.e., when business and technology are infused with the values of security as well as other privacy and confidentiality concerns at each stage of design and implementation. Unfortunately, that has never been the case with the Internet or with many networks that are required to modernize constantly while, at the same time, continuing to use legacy systems. The issue is not just a matter of policy, but of practicality.

As the Defense Science Board made clear, "The Global Information Grid is a weapons system and must be treated as such. The United States is in an arms race, and experience suggests that as U.S. defensive capabilities increase, so will the adversary's offense… There is currently no security or Information Assurance architecture planned that addresses the emerging threat."[8]

History

This lack of an Information Assurance (IA) architecture is not for want of trying. As far back as 1998, President Bill Clinton signed Presidential Decision Directive (PDD) 63 that addressed the need to protect the nation's critical infrastructure that is defined as:

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked."

In 2003, President George W. Bush announced the National Strategy to Secure Cyberspace which had three strategic goals:

- Prevent cyber attacks against U.S. critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.[10]

The plan identified the following eight major priorities:

- Establish a public-private architecture for responding to national-level cyber incidents;
- Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;
- Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;
- Expand the Cyber Warning and Information Network to support the role of the Department of Homeland Security (DHS) in coordinating crisis management for cyberspace security;
- Improve national incident management;
- Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;
- Exercise cyber security continuity plans for federal systems; and
- Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.[11]

As a result of the plan's creation, much has been done to drive forward on these eight priorities. There are regular exercises to test the government's continuity plans, and DHS is playing a central role in coordinating the national effort which does involve improved public-private information sharing. However, there is a general recognition that even if the plan is fully implemented, the United States will remain critically vulnerable to attack.

Vulnerabilities and Threats

Historically, warfare has been a way for governments to acquire territory and elements of national power, including economic assets, through the use of force. One key in this concept is control of information which can be used to create and sustain legitimacy. A second vital element is that of technology, particularly as it relates to control of intellectual property. Traditionally, control of these levers of power have been managed through the use of armies, and significant resources have been expended down the centuries in using technology to seize advantage on the battlefield, from the development of the longbow to the horse, the rifle, the tank and the smart weapons of today. But the vast majority of economic and technological power resides entirely in the private sector, and it is an impossible task for the government to effectively control something it does not own with information and technology it either doesn't share or doesn't have.

Today, the need to deploy armies to achieve power has diminished significantly. For example, the cyber realm provides the opportunity to seize technology and economic power through the wholesale theft of intellectual property which reduces the economic, political and military effectiveness of the U.S. in the world. It is vital, then, that there is a public understanding of the cyber environment where vigorous debate could deliver an overall strategy for the nation. That debate can only occur where there is leadership that encourages true collaboration and a move away from the more traditional posture of "them" (the private sector which will do what they are told) and "us" (the public sector that holds all the levers of national power and can pull them at will).

At a veterans' conference in March 2008, Gordon England, the Deputy Secretary of Defense, acknowledged that the United States is already engaged in a cyber war. "It's one of our major challenges," he said. "I think cyber attacks are probably analogous to the first time, way back when people had bows and arrows and spears," he continued, "and somebody showed up with gunpowder and everybody said, 'Wow. What was that?'"[12]

The computer generation has created a new battlefield in cyberspace where the weapons are not bullets and bombs, but bits and bytes. Today, no massed armies are needed to seize economic value, and significant cyber real estate can be gained without firing a shot. Cyber offers adversaries a classic "Economy of Force" option that also packs a big economic and military punch.

During the Cold War, it seemed so much simpler when battle lines were clear and the enemy soldier wore a uniform and advanced with a weapon across a battlefield. Today, the attacker can be thousands of miles away and may be a government employee trying to harm another nation using highly sophisticated computer technology. Alternatively, he or she might be a disgruntled civilian using technology bought at a local computer store. All of this is done anonymously, greatly reducing the victim's ability to know of the attack, let alone who attacked and why they attacked.

This blurring of the battle lines between the public and private sectors - some might even argue loss of distinction between nation states and non-state actors and between what the intelligence community knows and what the private sector knows and what the other party needs to know (not everything, just more than it does today) - has created extraordinary gaps in the nation's visibility over information technology infrastructure.

Among the attacks that have been disclosed publicly:

- There are more than three million probes of government networks every day.[13]
- There were 37,258 reported attacks on government and private networks in 2007 compared with 4,095 in 2004.[14] There were nearly 13,000 direct assaults on federal agencies that same year, and 80,000 attempted computer network attacks on Defense Department systems.[15]
- The attempted theft of 'quiet drive' technology for the latest generation of U.S. submarines.[16]
- The hacking breach into the computer network that supports Robert Gates, the U.S. Secretary of Defense.[17]
- There are 120 countries currently engaging in active Information Operations.[18]
- According to a survey on the economic cost of cyber attacks worldwide conducted by the U.S. Congressional Research service: "The 2003 loss estimates ….range from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks)."[19]

- In August 2006, the SysAdmin, Audit, Network, Security (SANS) Institute claimed that bank's financial losses caused by cyber attacks were up 450% from the first half of 2005.[20]
- In December 2007, the head of MI5, Britain's equivalent of the FBI, sent an unprecedented letter to the CEOs of 300 leading British businesses warning them that they were under attack by "electronic espionage."[21]
- In May 2007, a wave of data attacks against Estonia, which was thought to originate in Russia, closed down the country's newspapers, the major bank and many government departments.[22]
- In August, 2008, a wave of cyber attacks from Russia disabled Georgian government websites in advance of the Russian invasion of South Ossetia. [23]

While significant steps have been taken over the past decade to impose cyber standards,[24] improve the education of network managers and raise awareness in the public and private sectors, it is still a fact that any defensive line remains full of holes, due in large part to a lack of a unified, cohesive strategy. As the Pentagon's Defense Science Board reported in 2001, "DoD is vulnerable…there are several operating systems in use and in excess of 700 applications – all collectively using greater than 100 million lines of software code. Few of these have been checked for malicious code and new hardware and software is installed virtually every day."[25]

The convergence of technologies and connectivity that links everyone across the globe, while enabling increased communications and exchanges, also creates increased vulnerability. A virus planted on one continent can spread in seconds to another continent and then across the globe. This means that no nation can stand alone and expect to create an effective defense against possible attacks. The vulnerabilities of the current global information infrastructure have proved an irresistible target. In the past decade, the threat matrix has transformed from amateurs doing their best to prove they were smarter than the system, to billions of dollars of organized criminal activity, to massive information warfare efforts and investments by nations.

Additionally, this convergence of technology and increased connectivity is compounded by the problems associated with significant legacy systems that cannot be brought up to standards easily, as well as the complex inter-dependencies between software vendors that make it difficult to address security problems without damaging the intended functionality. These factors make the problem of mounting an effective defense of the network extremely complex.

Both Moonlight Maze, a series of attacks against government and other networks that appeared to come from Moscow,[26] and Titan Rain, a series of thousands of attacks against the public and private sectors in the U.S. ,[27] are examples of state-sponsored attacks on a wide scale. They are illustrative of the growing complexity of the attacks and the sophistication of the attackers which make detection ever more difficult. As the appreciation of the asymmetric opportunities of cyber attacks has spread to other nations, so other countries have developed their own capabilities.[28]

With this expansion of the cyber threat, it has become increasingly difficult to distinguish between different attackers or even to identify where the attacks originate. An attack that seems to be coming from an individual or a fringe group might, in fact, be state-sponsored, and an attack that seems to originate in Moscow might, in fact, begin in Paris.

By 2006, IBM's Global Business Security Index was able to predict an evolving and threatening environment on the Web, which included:

- **Insider Attacks** - As software becomes more secure, computer users will continue to be the weak link for companies and organizations. Criminals will focus their efforts on convincing end users to execute the attack instead of wasting time in lengthy software vulnerability discovery. Global resources, employee layoffs, and mergers and acquisitions all present challenges for companies and organizations attempting to educate users against these threats.

- **Emerging Markets** - Cyber criminals take advantage of poor international cooperation against cyber crime and launch cross-border attacks with little personal risk, so the threat to and from emerging and developing countries is therefore increasing. It then becomes far more difficult to trace the attacks back to their source, especially when trends show that attacks are increasingly originating from regions such as Eastern Europe and Asia, where sanctions are more lenient and enforcement is limited.

- **Blogging** - The increased use of collaboration tools such as blogging increases the possibility of leaking confidential business data.

- **Instant Messaging** - Botnets, a collection of software robots that allow a system to be controlled without the owner's knowledge, will continue to represent one of the biggest threats to the Internet. Newer botnets, which will have smaller cells in order to better hide, will likely move to instant messaging and other peer-to-peer networks for command and control of infected systems.

- **Mobile Devices** - Malware[29] affecting mobile phones, PDAs and other wireless devices has increased substantially in the last year, but has not materialized into pervasive outbreaks since they cannot spread on their own - yet.[30]

The National Academy of Engineering recognized the difficulties of the cyber world when it announced that securing cyberspace ranked among the top 14 challenges confronting the world, alongside such other complex and challenging issues as reverse engineering the brain, enhancing virtual reality and managing the nitrogen cycle.

"Electronic computing and communication pose some of the most complex challenges engineering has ever faced. They range from protecting the confidentiality and integrity of transmitted information and deterring identity theft to preventing the scenario recently dramatized in the Bruce Willis movie 'Live Free or Die Hard,' in which hackers take down the transportation system, then communications, and finally the power grid.

As that movie depicted, networks of electronic information flow are now embedded in nearly every aspect of modern life. From controlling traffic lights to routing airplanes, computer systems govern virtually every form of transportation. Radio and TV signals, cell phones, and (obviously) e-mail all provide vivid examples of how communication depends on computers — not only in daily life, but also for military, financial, and emergency services. Utility systems providing electricity, gas, and water can be crippled by cyberspace disruptions. Attacks on any of these networks would potentially have disastrous consequences for individuals and for society."[31]

Part of the challenge is the sheer complexity of the systems involved. Complexity theory shows that beyond a certain threshold the number of test pathways becomes infinite. This means that, even when the test environment is stable – which is not the case in today's cyber environments – it is impossible to test every possible pathway into the system. The best approach, therefore, is to automate vulnerability analysis, inspect and verify code and architecture at every step, and operationally defend the system.

Despite the obvious truth of mutual and shared vulnerability that has come with the blurring of the battle lines in the cyber world, both the public and private sectors see themselves as separate. In many foreign countries, the national Intelligence Community (IC) can and has been used as a national asset to provide information to the business community on competing bids for a contract or to interfere with a competitor's ability to compete. In the United States, the intelligence community is legally constrained from such activity. At the same time, some in the IC see little reason to put sources and methods and people at risk to protect a business and its shareholders. In addition, companies do not trust that governments can keep their secrets, and worry that shareholder value would be compromised by the sharing of data on incidents, intrusions, attacks or vulnerabilities.

This separation of power and responsibility in the United States helps make the country uniquely vulnerable. It is no coincidence that each country that is most successful in attacking the United States through cyberspace has a centralized government that has significant control over the private sector; what they steal directly benefits their economy. The United States loses intellectual property that in turn diminishes our competitive advantage and severs the connection between investment and return that provides incentive for innovation.

As the world has become more networked, vulnerabilities have become shared. For example, significant efforts have been made by potential enemies of the United States to tap into the unclassified computer networks that support the logistics infrastructure that would allow the United States to go to war. Further, the private sector and industrial base are experiencing an onslaught of attacks at the same pace. Newer attacks are targeted and consequently not just going unnoticed, but even when detected, are going unreported. Thus, the risks are poorly managed. These same types of attacks on U.S. commercial power grids or water supplies could quickly prove devastating and cause significant loss of life. The shared vulnerabilities of both the public and private sectors pose great risk to our country.

The Hydra Conundrum

The consensus in the IT industry is that Moore's Law, which observes that computing power per dollar doubles every 18 months (i.e., increases 1,000-fold every 15 years), will remain true for another decade, if not longer.[32] Therefore, information and technology vendors must continually innovate just to maintain their market position.

At the same time it improves performance, the IT infrastructure must also be more secure and resilient – characteristics that are superficially deemed to be in competition with each other. This creates a natural tension in the IT environment where the demand for increasingly lower cost and higher performance technology can be muted by the added cost and slower performance of related security and resilience features. The evolution of technology systems driven by the availability of new, lower cost and higher performance components, means that change is more rapid – what was thought impossible last year, becomes possible this year. Hackers who exploit this weakness create vulnerabilities and threats. As soon as one threat or weakness is developed, another emerges, rather like the Hydra in Greek mythology who would grow back two heads for every one that was cut off. Further, given the inadequacies of the current governance structure, threats and weaknesses that are identified, in fact, may not be addressed, thereby contributing to the current state of affairs – lack of appreciation for the severe nature of the current threats and lack of effective business processes to remedy them. This disconnect between detection and remedy requires attention by the commercial sector, including the IT industry, as well as government.

Although the United States arguably leads the world in information technology innovation, the last 10 years have seen a revolution in how that innovation is brought to market. It used to be the case that when a U.S. company sold a hardware or software product to the IT sector, it could be trusted as a reliable resource that was made in the USA. Today, the IT manufacturing value chain is globally distributed and the origin of components and software code is often a mystery to the purchaser and even unknown to the supplier.

Innovation is happening so fast and is so costly that every software and hardware manufacturer must seek the least expensive source for raw materials, components, and code. That means outsourcing overseas where labor costs tend to be lower and, certainly in the case of software, shipping costs over the Web are the same from India, or San Francisco. The fact that many of the best outsourcing resources reside in countries known to be conducting cyber espionage on a broad scale adds to the challenge. One estimate suggests that there are 15 million software coders in the world and that only half of them live and work in the U.S. It is expected that over the next few years the number of programmers in India, Brazil and Russia – all countries heavily engaged in information warfare (IW) – will increase at a faster rate.[33] Clearly, all programmers do not engage in IW. However, in China and India, both countries with a significant IT and IW capability, a total of 533 million people speak English, a significant resource for both governments.[34]

There are basically three ways that a competitive business or government can conduct espionage or sabotage. The first is by inserting a harmful device or piece of code at the source, while the product or software is being created. While this is easy to do, it is also the most risky because competent companies or organizations with effective governance may run checks to try and eliminate such risks. The second is to use a trusted insider to insert software into a system that is already up and running.

The third, and perhaps most important, opportunity comes from the rapidly evolving technology environment. Every piece of software requires routine updates, and many individuals and organizations choose to update hardware and software regularly. For example, any user of an operating system may be prompted frequently to download updates. For most people, such a download is routine, and yet it is a very simple software task to fake the source of the download, disguise it to look like a legitimate product and install a piece of malware inside an existing network.

Trusted Security

Many of the standard software services used by U.S. corporations and government institutions are created or derived from international sources and many control their particular market. Some countries regularly infect both hardware and software with viruses or malware that can be used later to steal information or compromise a network. If there were a closer sharing of information between communities with mutual interests, what is known about such threats and vulnerabilities would be accessible to all to the benefit of all.

"Increasingly when you buy computers they have components that originate … all around the world…We need to look at … how we assure that people are not embedding in very small components … that can be triggered remotely," said Michael Chertoff, the Secretary of Homeland Security.[35] Yet, exactly which countries and companies do this is neither known generally among government departments outside the intelligence community nor in private sector companies.

Although the U.S. led the early days of the information revolution, the country has fallen increasingly behind as the revolution has gathered pace. This is most evidenced in the education system where the quality of academic instruction on security is generally low and there is very little effort to teach students about secure coding, the value of a secure architecture, and the need for security controls and ethics. In general, the importance of security has not been adequately socialized. While automated quality assurance may help, this lack of competence encourages companies to outsource overseas and contributes to putting the nation at a significant competitive disadvantage.

Because rigorous quality assurance capability is generally lacking in the industry, a number of proxies and surrogates are generally used to provide rough assessments. The most widely used system for quality assurance is Carnegie Mellon's Software Engineering Institute's family of Capability Maturity Models (CMM and CMMI, and the related ISO 9001), which measure organizational capability.[36] Can the organization reliably and repeatedly produce software within given estimates of cost and schedule? A CMM evaluation results in a rating on an integer scale from one (non-repeatable process) to five (measured and optimizing process). A CMM five rating is very difficult to achieve. High CMM ratings refer to process and organizational attributes. Most companies possess some kind of CMM level rating and are required in many U.S. government RFPs to have a rating in order to bid on a contract. Yet, there are no actual assurances regarding code produced or services offered.

Another set of standards has been created by the Center for Internet Security (CIS), a nonprofit whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS members develop and encourage the widespread use of security configuration benchmarks through a global consensus process involving participants from the public and private sectors.

The practical CIS Benchmarks support available high level standards that deal with the “Why, Who, When, and Where” aspects of IT security by detailing “How” to secure an ever-widening array of workstations, servers, network devices, and software applications in terms of technology specific controls. CIS Scoring Tools analyze and report system compliance with the technical control settings in the Benchmarks. The U.S. government has recently adopted the CIS Common Security Configurations and uses their CIS Benchmarks, Scoring and Audit Tools. However, the CIS standards do not work across interdependent systems, and government and industry leadership is needed to encourage practices that involve information sharing between vendors.

For security attributes, the National Information Assurance Partnership (NIAP) Common Criteria (CC), codified as ISO standard 15408, are relatively widely adopted. The CC, developed primarily by National Institute of Standards and Technology (NIST), builds on a long legacy of security evaluation processes. The CC process is complex and can be costly for a vendor. A high rating indicates that a system conforms well with the profile of systems in its category (e.g., a firewall, a desktop operating system, etc). It also indicates that the design of the system respects the security requirements. But it provides no actual assurances regarding code produced, for example, that it is free of vulnerabilities or even malicious capabilities. CC is a means to document the development process post production and to provide quality assurance, including vulnerability analysis at higher assurance levels. It is not a standard for security of software. Nonetheless, a high CC rating suggests that when vulnerabilities do surface, they can be repaired relatively easily.

In 2002, the U.S. Congress passed and the President signed into law the Federal Information Security Management Act (FISMA), which was designed to improve the cyber protections both within government agencies and with the contractors who serve them. Although FISMA raised awareness, many inside and outside the government view it as flawed in that it requires obedience to a process which does not itself guarantee security.[37]

For example, in one case, as part of the FISMA compliance process, a federal agency sent 1,000 employees to a security awareness training course, which they all passed. Four hours later, they were tested using a social engineering technique that is part of the exploitation process used in the Titan Rain attacks, and 800 of the people from the class failed the test.[38]

All these efforts have made some structural order out of the chaos but, absent effective governance, have not delivered the kind of rigor that is really needed. The legislative and executive branch efforts to legislate and then manage by executive order and regulation have not been entirely effective. Important differences between intent and implementation have resulted in lack of cohesion in governmental efforts. The legislative and administrative portions of the U.S. government have actually caused a disagreement in policy and practice on how to secure governmental enterprises.

For example, at an April 2007 hearing of the House Homeland Security Subcommittee on Emerging Threats, Cyber Security and Science and Technology, Representative James Langevin, the Committee Chairman reported that hackers using Chinese Internet servers launched an attack on the Commerce Department's computers in October 2006. "I think these incidents have opened a lot of eyes in the halls of Congress," said Langevin. "We don't know the scope of our networks. We don't know who's inside our networks. We don't know what information has been stolen. We need to get serious about this threat to our national security."[39]

At the same hearing, Greg Wilshusen, the director of the Government Accountability Office (GAO) Information Security Issues division, argued that there is a significant difference between being FISMA accredited and having security that works. "Just performing certain activities doesn't mean they are being performed effectively," he said. "Just because a system is certified and accredited does not make it necessarily secure."[40]

A recent study by the GAO found that "significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets and personnel of federal agencies." In their fiscal 2007 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information security controls were either a significant deficiency or a material weakness. GAO audits returned similar findings for financial and non-financial systems.[41]

Among security experts, both in contracting companies that supply services to the government and in government agencies themselves, there is considerable cynicism about the effectiveness of FISMA.[42] While FISMA law is clear, in effect, agencies have the ability to choose between an evaluation against a subjective standard and a third party audit for which there are more rigorous standards.[43]

In its 2007 report, the House Government Oversight and Reform Committee gave the 24 government agencies covered by the report an overall grade of C- for compliance to FISMA in 2006, up from D or D+ the previous year. Eight agencies received an F and six agencies got a worse grade than the year before. Clearly, something is not working in the FISMA process.[44] Equally, while FISMA requires all government technology suppliers to be compliant, few agencies enforce the rule, and so potential breaches in the technology and software architecture are created from the inception of a contract.

Unlike the Cold War, with its highly developed war fighting and peace making architecture and deterrence strategies, all of which were based on a broad and deep public discourse, the evolution of the cyber world of offense and defense has been largely hidden behind a veil of secrecy and has occurred over a comparatively shorter period of time. As a result, failure can be hidden, debate stifled and intelligence unshared with the exposed and the vulnerable. It is time for a more transparent process among a broad range of stakeholders that will serve the nation to greater effect.

It is clear that despite the efforts of the government and the private sector, the existing process for cyber defense is not working. There are simply too many holes in the process and in security products while the proliferation of attackers and their growing sophistication means that any gap is exploited quickly.

What is needed next is a new conceptual framework to organize the complex elements of cyber into a coherent whole – one that can be used to explain and organize the complex features of the cyber world into a unified architecture. And one that stakeholders with disparate interests in the cyber world can embrace.

Understanding Cyber in the Context of Other Global Movement Systems

Since 2005, IBM has sought to help clients improve the security, performance and resilience of complex systems using a framework known as Global Movement Management (GMM). The GMM framework starts with the recognition that the global movement of people, goods, cargo, money and information increasingly relies on complex and interdependent networks. These networks have grown over time in response to the demands of the global economy to provide goods and services with increasing efficiency. Global movement systems span international borders and are owned and operated by myriad actors in the public and private sectors. Global movement systems include the immigration system, maritime cargo shipping, international aviation, international banking, and the Internet.

All of these networks pose similar benefits and challenges. They are the "dial tone" of the modern global economy, providing the goods, services and information that comprise the stuff of daily life. People rely on these networks, and indeed have an expectation that these networks will work. A disruption to any of these networks can have unpredictable and large-scale economic consequences. At the same time, these networks can be intentionally exploited or targeted for malign purposes. Drug cartels can use international immigration flows as channels for the drug trade. Terrorists can legally exploit immigration systems to enter countries that are the target of their attacks. The maritime cargo system could be exploited to deliver a nuclear device into a country. Airplanes and hazardous chemical shipments can be targeted and harnessed as weapons.

The risk posed by global movement systems lies not only in the ability to use them for malicious purposes. Risk is also created by the enormous level of uncertainty, unpredictability, and asymmetry posed by the increasingly networked nature of the global economy. For example, the U.S. auto industry was shut down when a strike closed the port of Los Angeles in the fall of 2002.[45] The 9/11 attacks cost less than $500,000 to plan and execute, but resulted in the effective shutdown of the entire U.S. aviation system and caused $80 billion in damage.[46]

Global movement systems are both a strength and weakness of the global economy of which cyberspace is a central part. The Internet and the increasing reliance on digital data and networked computer systems make governments and companies more productive. Basic economic flows rely on companion flows of digital information. At the same time, they pose the kinds of risks discussed at length in this paper – the use of the Internet by terrorists, by criminal syndicates to raise money via fraud and identity theft, by national governments as a tool of espionage and information warfare, and the potential to use cyber methods to instruct Supervisory Control and Data Acquisition (SCADA) systems to inflict damage in the physical world by targeting, for example, electric, oil, gas, and water facilities.

The following section will review the basics of the GMM framework and use them as a guide for how to begin to address the complexity of the challenges presented in cyberspace. The use of GMM to frame the cyber security challenge will help achieve two important things. First, GMM can aid in simplifying the complex topic of cyber security, hopefully making what many consider an arcane topic much more accessible to general audiences as well as policymakers. Second, by facilitating increased transparency and understanding of the complex cyber challenge, GMM can serve as a catalyst for developing the right strategies and solutions that allow maximization of economic and national security benefits from reliance on cyberspace while minimizing the risks. This means developing a strategic approach to cyber security in which security and commerce are not mutually exclusive ends, but mutually reinforcing goals.

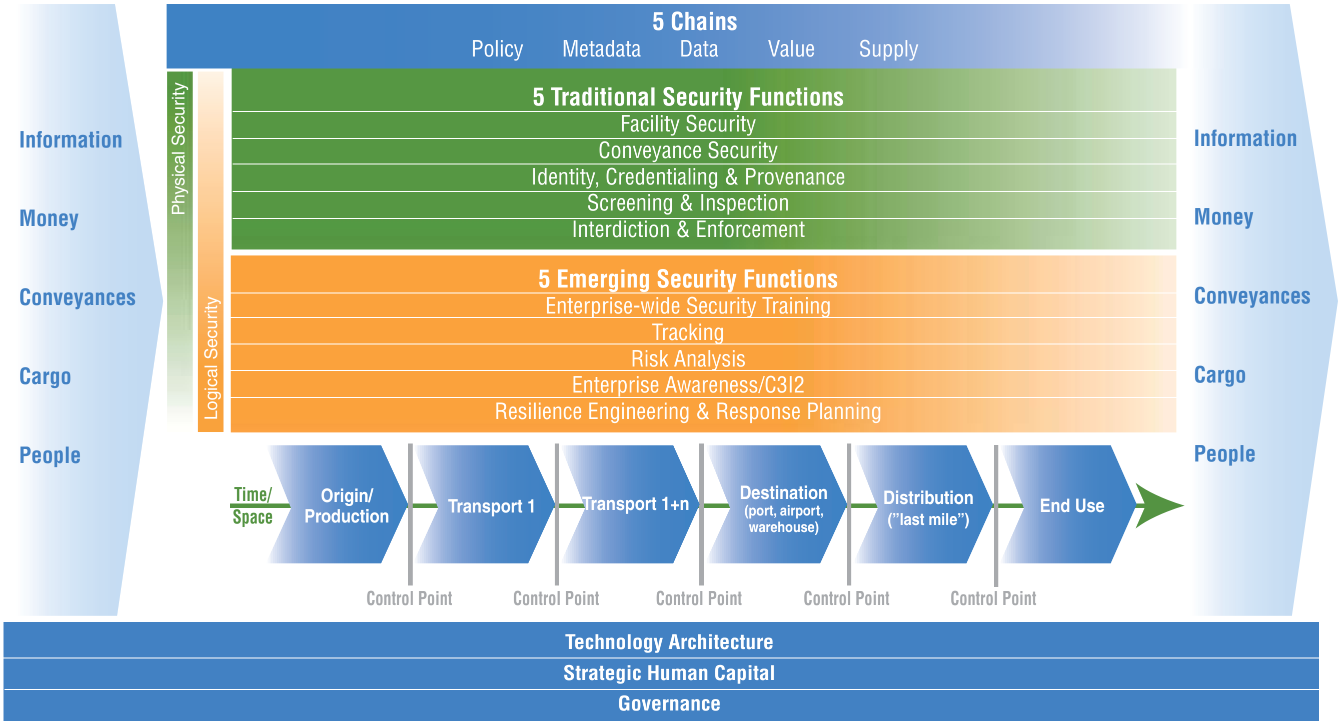
Overview of Global Movement Management

A principal tenet of the GMM framework is that all flows in the global movement system are more alike than they are different, and that these similarities hold the key for developing policies to strengthen the security, resilience and performance of such systems. Within the GMM framework, all complex flows in the global economy – people, cargo, conveyances, money and information as depicted on the left side of Figure 1 – can be analyzed using a common analytical approach that relies on the combination of two methodologies. The first is a “component business model” which is used to decompose even the most complex system into its component parts. The second, a “supply chain model,” is used to describe any complex system as having as a basic purpose the goal of moving objects – bits, bytes, shipping containers, travelers, airplanes – from point A to point B.

While “supply chain” refers to “physical goods,” there are in fact many parallel chains. The “value chain” reflects the flows of money and value that often trace the movement of physical goods. The “data” and “metadata” chains reflect the flows of information that trace the movement of goods and money. And the “policy chain” reflects the collection of rules and behaviors that accompany the movement of goods, money and information.

Used together, these methodologies allow any movement system to be depicted as the generic movement system at the center of Figure 1. As any object moves from “origin” to its ultimate destination “end use,” it moves via different modes of transport and through various control points where it is stored and kept.

Figure 1: The GMM Framework



It is at these different levels – object, storage, transport and enterprise – that owners of movement systems seek to implement security measures. Security measures can take many forms. These start with the most basic and traditional measures, like installing a gate around a warehouse (facility security) and requiring employees to prove their identity and employment history before being hired (identification and credentialing). They also include measures which require more planning and forethought and which have dual benefits beyond simple security, such as employee training, resilience engineering, enterprise risk analysis, and response planning and exercising. This full range of options is depicted by the orange and green bars in Figure 1. No one security measure will ever be foolproof or perfect, but when layered together, multiple security measures, no matter how imperfect each one, will increase the overall security of any system and allow business and government leaders to reduce risk enormously in a way that is cost effective and can create not just better security, but also benefits to core business processes. This process is called layering.

Finally, the effectiveness and efficiency of any security regime rely on three major levers: human capital, technology, and governance, as depicted by the blue bars at the bottom of Figure 1. People do their jobs better when empowered by the right technologies and clear rule sets. Technologies do not improve security if they complicate the jobs of front line employees and decision-makers. Governance that creates such strict rules that creativity, innovation and initiative are frowned upon will create a brittle corporate culture that will not respond well to crises. Only when human capital, technology, and governance are viewed holistically can critical movement systems like cyberspace by made both more secure and resilient at the same time in a way that can also improve overall performance.

Applying Global Movement Management to Cyber

The traditional link between cyber and real-world commerce is obvious. International commerce and travel increasingly rely on electronic data to improve tracking and delivery of people and goods and to facilitate financial flows and the settlement of payments. The link between cyber and security has been heightened since 9/11 as international security efforts rely increasingly on access to digital information to gauge the risks posed by cargo and passengers and to detect crime, fraud and terrorism. The public has become increasingly aware of the gravity of threats posed by cyber, including the threat of computer viruses, identity theft, and fraud. Fewer people are generally aware that SCADA digital control systems for public utilities can transform crimes in the virtual world into crimes that can cause physical threats to dams, waste and drinking water, and energy supplies including oil, gas, and the electric grid. And while many people are familiar with the notion of cyber warfare, very few are generally aware of the massive scope and scale of cyber attacks and information warfare that are taking place everyday. It is this ever-increasing threat that led to the recent presidential cyber security directive.

Cyber security involves the protection of digital information and the systems on which digital information travels and resides, and includes a wide range of software and hardware, as well as design and behavioral aspects governing how people interact with data and IT systems, and how data and systems interact with other data and systems. Securing cyberspace entails implementing security measures at multiple levels. At the level of individual objects, encryption (SSL, PKI, etc.) can help secure individual records within databases, packets of data in motion, or the contents of emails. Individual computers, individual files, and individual applications are examined and scanned with antivirus software.

To protect stored data, access to individual computers and individual systems is protected by firewalls. Electronic access to systems and from systems are secured using such tools as e-mail authentication, URL filtering, spam filtering, and content monitoring and filtering. Human access to systems is made secure via user authentication, authorization management, single sign-on, passwords and password authentication methods, and biometric technologies. Proper access is further assured by business rules that establish clear role and authorization management for who has access to what data and what systems under what circumstances. In addition, things like anti-phishing measures help prevent individuals from inadvertently disclosing passwords to malicious actors.

At the transport layer, networks are made secure using network access controls and virtual private networks. Other security measures allow mirroring and backing up data, disposing of data according to predetermined data retention policies, and distributing data across multiple nodes. Still other measures include audits, network behavior analysis and database activity monitors to detect fraud and other anomalies. And, automated and human probing of behaviors, networks, systems and interconnections can assist in identifying and managing vulnerabilities. Fixes to known vulnerabilities are regularly implemented with patch management.

In addition to implementing security measures at each individual level of networked IT systems (object, storage, and transport), cyber security also relies on the coordination, interaction, and synergy of security measures layered at multiple levels in the enterprise. It is also worth noting that over time security measures often migrate in either of two directions. What might have been sold as point security products at one point in time can become commoditized. Over time, many basic security features become embedded in IT infrastructure or within operating software. This explains the acquisition of security companies by large hardware and software companies who view the integration of greater security features as a necessary means of staying competitive in the marketplace. Security offerings can also migrate upstream, so that companies can choose not to own and operate certain security solutions, but rather acquire certain security measures as part of a managed services offering provided by a third party provider.

Further, a healthy cyber system is one that is characterized by the GMM concept of “intelligent immunity.” Intelligent immunity is an end state of the cyber system defined by layered security, enterprise awareness based on real time information flows and anomaly detection, and resilience in the face of attacks or misuse. Setting intelligent immunity as the goal for global movement systems allows a calibrated, layered, and flexible approach to security that seeks to improve the overall health and well-being of the system. It does so by strengthening resistance to attack while avoiding actions that impede growth and every-day commerce.

In the face of attack, the global system has to marshal defenses in an immediate but discriminating response, but also take preventive action. Security measures must shut down only the affected areas and swiftly repair and recover to normal functioning. And, there must be a memory component so that threats are more immediately recognized and addressed over time. With each attempt, the system becomes more intelligent to stave off future threats.

Given the above context, the GMM framework applied to cyber security can assist in successful implementation of the U.S. cyber initiative. The national response should be developed, organized and executed in a way that will deal with the scope, scale and complexity of the threat while ensuring a commitment to privacy. It should support a high level of integrity where individuals and organizations can expect data communication networks to be secure and “always on.”

Elements of a New Cyber Framework

In the past 10 years, definitions of critical infrastructure, cyber space, and cyber defense have evolved so that now there are multiple interpretations within the public and private sectors. This paper has outlined a simpler and more easily understood cyber framework that will help organize an effort to protect the nation's entire electromagnetic spectrum including computer systems and infrastructure to ensure essential information is secure. The goal of this effort should be to create a more efficient, secure and resilient global cyber system.

A cyber framework is designed to protect the nation's entire electromagnetic spectrum, including computer systems and infrastructure, to ensure essential information is secure. This will be achieved by creating a more efficient, secure and resilient global cyber environment that respects societal norms like privacy and confidentiality through the effective use of tools including international agreements, deterrence, business processes and technologies.

To implement the framework there is a need to take a risk-based approach to improve the performance, security and resilience of the system. This means that not all systems need protection, and that the cost of creating higher levels of performance, security and resilience should be considered along with the benefit in both economic and societal terms. One example of a possible risk-based approach that might be applicable to the cyber arena is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) (method, approach, technique) that is a generally accepted approach for Sarbanes-Oxley Act oversight and risk management requirements.

A framework to make effective use of the people, technology and governance systems available today should include the following elements:

- Leadership
- Governance
- Civil Liberties and Privacy
- Deterrence
- Cyber Security Treaty
- Balanced Defense and Offense.

Additionally, there are other considerations that will inform this framework, such as legal liability, law enforcement, and strategic human capital. Each of these is discussed below.

Leadership

Over the past decades, a number of initiatives to manage the cyber environment have come and gone. These efforts have been aimed at improving network, software and hardware security and imposing a set of processes designed to improve implementation and monitoring. Throughout this lengthy process, there has never been a single place in either the public or the private sector where individuals, companies or agencies could go for advice. There remain no effective methods of accountability should any organization in the information value chain fail to deliver on any standard.

Lacking coherent leadership, it is inevitable that standards are interpreted differently throughout the government and the private sector. Today, every intelligence agency runs its own, largely independent cyber plan augmented by frequently competing plans among the single services, and all are formed and executed without a coherent process of governance. The result is somewhat like the early days of the space race when everyone was competing; there was huge inefficiency, overlap and waste, and no agreement on who should actually drive the process forward in a coherent and effective way.

Paralleling the continuing IT revolution in the private sector, the Pentagon is driving a process to modernize its information technology. The Air Force has established plans for a new Cyber Command which will be the most ambitious effort yet to centralize communications and security. The Navy will announce plans later this year for a Next Generation Enterprise Network to serve users worldwide. The Army has a separate plan underway to establish two area processing centers designed to improve information security.[47]

President Bush has decided to launch a major cyber initiative that involves a new multi-billion dollar budget spread over several years. As part of this initiative, the DNI plans to establish the Single Information Environment for the intelligence community,[48] which will have six components:

- **Network Convergence.** Reducing the number of network connections to 50 from the current several thousand while introducing three fiber networks: one for unclassified, one for classified and the third for Top Secret.[49]
- **Common Software Environment.** Instead of every agency developing and buying solutions on its own, a single agency will buy an application that must work across the other 15 agencies of the community.[50]
- **Enterprise Licensing.** Instead of one agency licensing software, the buying power of 16 agencies will be used to leverage better economies to enable common business processes.[51]
- **Global Email.** Currently, the IC is stovepiped into different email silos. This will allow global communication. [52]
- **Data Center Consolidation.** Different agencies have many different data centers, but a common structure and shared data centers will reduce redundancies. [53]
- **Common Desktop Environment.** Any member of the IC will be able to log-on to any computer within the IC and work as if he or she is back at the home office.[54]

But there is much more to meeting this challenge than the DNI imposing a different structure on the government's IC information management. Even this limited effort seems to have a challenging future as different parts of the intelligence community have already made clear that their special needs will require them to be excluded from much of the new process. Also, this only deals with the intelligence community. The rest of the government is still on its own with guidance from the White House and OMB now emerging, and improved efforts among civilian agencies and the private sector emerging, but no evident enforcement mechanisms in place.

Missing from the DNI's list is anything beyond the organizing of the bits and bytes into a more coherent whole. Without standard setting, effective governance and strict measures of accountability, changing the organization of the bits and bytes will achieve little. The list must be matched with effective governance over the cyber environment involving 16 different intelligence agencies and every branch of the armed forces. This is hardly surprising given that the computer age is being imposed on a structure that was largely created after World War II before computers were in widespread use.

The President's cyber initiative has already run into practical and legal constraints. The DNI is crafting the cyber strategy for parts of the government, but the Department of Homeland Security has much of the critical legal authority to execute the program inside the U.S. From DHS, money will be dispensed to other parts of the intelligence community and law enforcement. Meanwhile, DoD will continue to control and manage its own cyber budget. The President's recent cyber initiative is a start in the right direction but needs to go further.

It is time for a new and innovative leadership approach for the cyber community that involves both the public and private sectors, a coordinated approach that will allow standards to be set, civil liberties protected and a nation defended effectively. The question is what effective leadership might look like and how that leadership can be effective in two sectors with very different interests. The approach must engage all of government, not just DoD and the intelligence community, as well as the private sector. The government participants can help set standards and make recommendations in collaboration with the private sector as well as create incentives for adoption through the contracting process.

The independent private sector has made clear its reluctance to share information with a single government entity without absolute guarantees that any information will remain secure and not subject to the Freedom of Information Act. The private sector will resist government efforts to impose standards that they fear will stifle innovation and reduce international competitiveness. The answer to those real fears lies in leadership across the sectors that can develop requirements for the public sector and inspire adoption by the private sector using its purchasing power and standard-setting influence.

The reality is that the majority of the large U.S. high technology corporations do most of their business with the private sector and are global companies, so government work is a minority interest. At the same time, governments tend to see companies that are headquartered on their territory as “American” or “British” companies, which does not reflect the market reality. Understanding this is central to finding a way forward to better cyber security. A government-mandated solution that only takes account of government interests will not work and could do serious damage to the companies on which the government depends for its own information technology needs.

Governance

Governance reflects the framework, principles, structure, processes and practices needed to set direction and monitor compliance and performance aligned with the overall purpose and objectives of an organization. The issue of governance touches several areas. One part of the standard must address hardware and software issues. Two models currently exist that go part way to a solution: The first is CIS, and the second is Carnegie Mellon’s CERT Coordination Center which acts as a clearing house for software vulnerabilities. However, neither is up to the task.

One of the principal challenges confronting anyone buying hardware or a new application is the inability to verify the information on the label of the box. It may look like a piece of genuine software, but there is really no way of testing whether the code is uninfected. Equally, a piece of hardware from a reputable company may seem valid, but hidden within it may be bugs that could do serious damage. Finally, software and hardware are updated all the time, and with software this is often done via a simple and automated download from the Web.

Currently, there is no effective way of validating the purity of the application, the hardware or the download. A new organization that sits between the public and private sectors - and independent from both - needs to be established to act as a hardware and software virtual vault where any enterprise could check what is being installed against a gold standard sealed in the vault. Software updates would pass through the virtual vault for validation as to source and compatibility before general distribution.

Below is another part of the standard that makes sense to consider (borrowing slightly from the SANS Institute (SysAdmin, Audit, Network, Security), a non-profit organization):

- "Change IT procurement from glossing over security in contracting to using the $65 billion in annual IT expenditures so that software and system suppliers and integrators have the right incentives to 'bake security in' to the systems they deliver to the government.
- Rewrite government standards and metrics from producing certification and accreditation reports that are rarely read, to monitoring 'attack-based' metrics that measure agency readiness to block attacks and to find and recover from attacks that get through the defenses. Make a unified approach to standards.
- Shift vulnerability management from flat scans that miss the techniques used by many of today's sophisticated attacks to pivot scans and penetration testing that closely resembles actual attack patterns.
- Move federal IT security spending from agencies writing meaningless allocations for security that are…ultimately used by project managers for contingency funds, to monitoring the specific allocation of security spending.
- Implement security automation transforms from manual patch testing and deployment to automated deployment.
- Transform defense and intrusion assessment from monitoring perimeter defenses to layered protection to identify and remediate attacks that have compromised the perimeter and to conduct 'deep-dive' analysis to find the footprints of attackers who have evaded all defenses."[55]

The challenge is that reliability is not just a government problem, but one that flows through all parts of the cyber infrastructure. Standards set by the government must also be acceptable to a private sector competing in the global marketplace where innovation and cost are key drivers. And to avoid exposure, both the public and private sectors need to be defended by a shield that begins with a process that deters all the likely attackers.

Civil Liberties and Privacy

The related issues of civil liberties and privacy must be considered as part of any significant cyber strategy. As was learned during the discussion of covert surveillance and other information gathering techniques after the September 11 attacks, there is deep distrust across a broad spectrum of the American people about the potential for government's intrusion in the private lives of its citizens.

Ironically, the individual American should be more concerned about attacks from criminals than from the government. Using automated software, organized criminals can hack into thousands of private computers to steal not just social security numbers but also online passwords and other personally identifiable information such as credit card numbers and the maiden name of an individual's mother.

As personal records have moved from paper to computer and the volume and variety of personal data has proliferated, so have concerns about the protection of data and the possible abuses that might occur by governments or organizations. These concerns have been fueled in part by the drumbeat of reports about data breaches that in the wired world can reach an unprecedented scale. For example, in May 2006, a laptop taken home by an analyst working at the U.S. Department of Veterans' Affairs was stolen with the confidential data on 26.5 million veterans stored on the hard drive.[56]

These civil liberties and privacy concerns are deeply felt and ignoring them will set up a confrontation between the government and the general public as well as the public and private sectors. Instead of waiting for the inevitable confrontation, the nation will be better served by creating a transparent process among Americans. With that transparency, a middle ground acceptable to all may be found.

Even a high degree of transparency of the processes used to address individual situations may not be sufficient to allay the fears of civil libertarians or of the business community who do not trust their government to keep their trade secrets. This can be alleviated to some extent by a clear commitment by legislators to placing a high priority on privacy and data protection, using such tools as data anonymization, 2-factor user authentication, immutable audits, and double-encrypted data, while enhancing the flow and quality of information shared. Only information required based on pre-defined events is published by the source systems and delivered to the authorized subscribers based on their requirements.[57]

Privacy can be protected best through a layered defense. This has to begin with strong data governance controls, limited data collection and controlled access at the beginning of the cyber dialogue. Data must be minimized and compartmentalized up front to answer the concerns of privacy loss.

With more effective governance in place, technology can come into play with the kind of point solution marketed by companies to control access to individual computers, up through companies that provide tools to protect data in motion as well as networks, and finally the protection of whole communities. Data security, which is a foundation of proper privacy controls, can be achieved via these layered measures.

But privacy and civil liberties in the end will only be achieved through a mixture of policies backed by legislation and adopted by agencies; a due process that is available to address individual mistakes or situations; oversight and accountability of the agencies that are using the information; and, imbuing agencies with a culture of respect for an individual's private information.

Deterrence

In his confirmation hearings before the Senate Armed Services Committee,[58] General Kevin P. Chilton, the current head of the U.S. Strategic Command described cyberspace as the new "emerging war fighting domain."

However effective the best defense, there is no doubt that some attacks will be successful. This means that the government needs to have, in addition to a resiliency plan, a pre-planned, graduated menu of responses that should be similar in form and substance to the Deterrent Strategy that was used so successfully during the Cold War. There are significant differences, however. Under the deterrent strategy known as Mutually Assured Destruction, there was recognition that a nuclear missile launched by Moscow or Washington would inevitably result in a massive counter strike. Both sides had clearly understood rules of engagement and a balance of terror was carefully maintained by the superpowers that controlled the nuclear triggers.

Today's Web world is anarchy by comparison. While there are laws, few users understand them and there are few, if any, real consequences for individuals or nation states behaving badly. While this is how the Web has evolved, and the constraints of the Cold War will never be replicated in the cyber environment, a measure of controlled response is desirable and possible.

Classic Deterrence Theory suggests that to be successful, a deterrent strategy has three key components: swiftness, certainty and severity.[59] In other words, any response to an act must be closely related in time to the attack itself, it must be clear in advance to the attacker that he is likely to be discovered and that punishment will be proportional.

But, there are certain key differences in the cyber world that make deterrence difficult to apply effectively. First, unlike missile attacks, there are few indications and warnings and most likely none of the damage that is so visible after a kinetic attack such as a bomb explosion. There might be very high economic cost, and the attacks could last months or even years and prove very resilient (as recent Russian and Chinese attacks have shown).

There is also a challenge in making a distinction between nation state activities, attacks by terrorist organizations, economic espionage or harassment by individuals. For example, there have been numerous instances of attacks that appear to come from one location that actually originate on a different continent.

The Department of Homeland Security has established the National Cyber Response Coordination Group (NCRCG), a forum of federal agencies that coordinates intra-governmental and public/private preparedness for large-scale cyber incidents.[60] In theory, the divisions between the different type of attacks – nation state, terrorist and individual – can be accounted for by the NCRCG being chaired by individuals from Defense, Justice or Homeland Security. The reality, however, is that an effective and calibrated response has not been established both within the government and in cooperation with the private sector. The organization is good at planning, but poor in responding to attacks.

An effective deterrence strategy depends on more transparent information sharing. An escalatory ladder of deterrence will rely on three separate communication components: business to business, business to government and government to attacker.

Business to Business: In this situation, an attack on one segment is communicated to another segment. For example, a bank that has been attacked tells a power company which tells a water company which tells a software company. Elements of this component include:

1. Identification of an attack and sharing of data within an Information Sharing and Analysis Center (ISAC) and the relevant business vertical. (ISACs have been formed in various business verticals such as banking to share information within the private sector).
2. Sharing of information across sectors.
3. Sharing of information with law enforcement.

Business to Government: In this situation, businesses that have been attacked (for example, a group of banks) tell the government. The government combines this report with information from other sectors allowing it to piece together a bigger picture of the attack. Elements include:

1. Identification of an attack that passes agreed thresholds (severity, technique or source).
2. Sharing of information with government with appropriate safeguards (anonymization of source).

Government to Attacker (including attacks on U.S. interests at home and overseas): In this situation, the U.S. government communicates directly with other governments when the attack comes from a second nation. Components of this strategy of increasing deterrents include:

1) Identification of attacks. Analysis by law enforcement, intelligence and DoD.

2) If seen as a criminal or civilian attack, law enforcement takes the lead through existing relationships with foreign police and intelligence.

3) If a nation state or state-sponsored terrorist attack, the lead may move to another federal agency, ranging from DoD, DHS, Department of Justice, State Department, or Office of the Director of National Intelligence.

4) Demarche. A diplomatic confrontation designed to encourage better behavior.

5) Publicity. A front page story in The New York Times setting out the complaint, identifying who is responsible, and the damage caused.

6) Sanctions. An economic consequence for causing economic damage.

7) Saber rattling. A warning that further consequences are inevitable unless the attacks stop.

8) Attack. This, too, has a highly calibrated list of options that might range from shutting down the computer in the office of a government official, to shutting down a network. As in kinetic energy warfare, this graduated response would be specifically designed to cause no loss of life until, as a last resort, the political leadership decided such a response was appropriate.

For a deterrent strategy to work, it must embrace the private sector because effective defense means defense for both the public and private sectors. For business, the Information Sharing and Analysis Centers are a useful beginning for intra-sector information exchanges, but the capability has to be expanded to run across all sector stovepipes and to embrace the knowledge gathered in the public and private domains. Ultimately, it will always be up to the government to manage law enforcement and effective deterrence, but the private sector has a vital and trusted role to play.

Cyber Security Treaty

Deterrence cannot work in isolation. Equally, for deterrence to be truly effective, all actors engaged in the process of defense and offense must understand the causes and effects of their actions. In the past, such behavior has been governed by international treaty. This is the appropriate vehicle for managing a new cyberspace regime.

In 2004, the Council of Europe enacted the first cyber crime treaty which has a series of guidelines and enforcement regimes for the 800 million members of the European Community (EC). As written, it principally protects data and allows for the prosecution of various cyber crimes.[61] While the EC approach is a useful first step, it does little to manage the international community where the majority of cyber criminal and warfare activity takes place. Forty nations have signed the treaty including the U.S. after the Senate ratified it in August 2006.[62]

During the Cold War, the Nuclear Non-Proliferation Treaty (NPT) and the less formal Missile Technology Control Regime (MTCR) brought together like-minded nations to control the spread of weapons that risked harm to all. Similarly, a Cyber Security Treaty (CST) could define common objectives and spell out an acceptable escalation regime in the global commons of cyberspace.

There is a current example that might provide some lessons learned for a CST. The Outer Space Treaty, or, as it is more formally known, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, was signed in 1967 and has been ratified by 98 countries.[63] This treaty is credited with keeping nuclear weapons out of space and created the basic framework for international space law.

There are significant incentives for international agreement on a CST. Every country believes that it is under cyber attack. So, if the United States were to take the lead in seeking a treaty, many countries would see it as a way of defending themselves. Also, many countries recognize that the current legal framework for dealing with cyber attacks is outdated.

According to a statement by Lt. Gen. William Campbell in a Hearing on Information Assurance and Information Superiority, “There is an urgent need for development and clarification of a legal framework that reflects the realities of the Information Age and the nature of cyber attacks. Deterrence, detection, tracking and identification of perpetrators will be very difficult unless the current legal framework changes. Currently, the laws do not favor the defender and greatly favor the attackers.”[64]

Balanced Defense and Offense

While all the capabilities outlined in the deterrent strategy above exist, the fact is that the vast majority of all cyber expenditures have been spent on defense, which has left the number and effectiveness of retaliatory options more limited. This is explained, in part, by the absence of a coherent national cyber strategy that spells out for the nation and the world the causes and effects contributing to action and reaction. Such a strategy exists for every other aspect of warfare and is well understood by the U.S. armed forces, the political chain of command and the nation’s enemies. A cyber strategy should be part of the nation’s defenses as well.

It is striking that in the context of warfighting, a cyber offensive capability represents a step change in the potential to deliver a precisely graduated weapons system to a very precisely delineated target to achieve a known effect. In the history of warfare through the centuries, such precision has never been possible before.

There are particular challenges around the implementation of any deterrent strategy that inevitably must involve offensive action. While it is possible to ‘track back’ attacks to their point of origin, some of these techniques are not reliable and are vulnerable to disinformation from the attackers.

These are complex issues, but they are exactly the kind of challenges that the development of a warfighting doctrine will address. The alternative is to do nothing and rely only on defense which the history of war suggests will be ineffective.

A study by the Potomac Institute for Policy Studies suggested that, among other criteria, an attack should be judged by its severity (i.e., if people are killed or if there is extensive property damage, the action is probably military; the less damage, the less likely the action is a use of force), immediacy (i.e., when the effects are seen within seconds to minutes – as when a bomb explodes – the operation is probably military; if the effects take weeks or months to appear, it is more likely diplomatic or economic), and directness (i.e., if the action taken is the sole cause of the result, it is more likely to be viewed as a use of force; as the link between cause and effect attenuates, so does the military nature of the act).[65]

Others have suggested that the United States should lead the world in creating, coordinating and implementing a “hot pursuit” policy that would allow for near instantaneous back tracking of attacks through cyberspace to their point of origin.[66] If standards for such a policy could be agreed upon, then the process by which an attacker is identified would be acceptable internationally and thus a deterrence strategy would have a degree of transparency that would make retaliation justifiable both in the court of public opinion and in a court of law.

While there are obvious differences between the public and private sector in cyberspace, there has been a long tradition of blurring those lines in law enforcement. For example, if an airliner is attacked by terrorists, the owner of the aircraft makes available all data to law enforcement who then takes responsibility for finding, arresting and trying the terrorist. A similar agreement could work well in the cyber environment.

The creation of a comprehensive cyber deterrence strategy will help clarify the distinction between defense, enabling tools for offensive capability, and offense itself. However, as part of the new transparency that needs to be included in the national and international discussion, it is important that real parameters are set that can engage the broad civil community and ensure a degree of trust about the process and its execution. In a kinetic environment, war is described as "just" in part when any response is proportional to the attack that provoked the retaliation. For example, an attack on a banking network that resulted in a $1 billion loss should not provoke a response that involved the raising of the gates on a dam and the potential loss of life downstream.

Not only must all responses be proportional, but they must be seen to be so. This means that a deterrent strategy must not only be known, but cause and effect will need to be discussed and defended in the court of public opinion. The cyber world is one where effective information management can quiet the anxious and calm the anarchy. Poor public relations could equally provoke an outpouring of offensive behavior that could make the initial attack appear insignificant by comparison.

Another challenging issue is the question of attack authority. In war, generals and admirals have rules of engagement that allow them considerable latitude in the conflict itself. In the cyber world, until now a U.S. offensive cyber capability is treated with the same degree of seriousness as the release of a nuclear weapon. While there are a range of options available to theater commanders, presidential authority is needed for most offensive acts. This is an immensely cumbersome and time-consuming process that takes no account of the more immediate world of cyberspace. A graduated deterrent must also accommodate a graduated and decentralized release process that reflects the severity of the response and the need for rapid response.

Other Considerations

While a strategy for cyber security must include a toolkit of options, those options must be vetted against certain criteria before adoption and implementation. The criteria should include the following:

Legal Liability

Two significant obstacles could prevent private sector companies from supporting the government's efforts in cyber security. First, current state and federal laws could be interpreted as prohibiting the very support the government needs.

Second, private sector companies could face significant third party liability from the targets of the government's cyber security efforts.

Current state and federal laws could be interpreted to prohibit assisting someone in accessing a computer in an unauthorized manner. If a U.S. technology company supplies a capability to a government entity and that entity then uses the capability to access a computer in an unauthorized manner, the U.S. company could be criminally liable for providing that capability. Second, the owner of the computer, or an individual with personal information stored on the computer, could hold the company liable for damages.[67] While the law remains unclear in this new realm of cyber war, it is already clear that companies are on the front line as the victims of cyber attack. It is logical to expect that they will also be on the front line in any legal actions taken to remediate damages incurred to their assets during an offensive attack in cyberspace. Both actions could have a devastating impact on the reputation, financial standing and future prospects of any business.

This must be overcome by a process of legal indemnity on the one hand and clear lines of demarcation drawn between what constitutes offense and defense. There is some precedence for this in the European Union's Cybercrime Treaty which was ratified in 2004.[68] The purpose of the Treaty was, in part, to address violations of network security and giving police powers to deal with computer-related crimes.[69] Although more than 30 countries have ratified the treaty, only a handful have adopted its framework into national law, so it remains essentially a toothless treaty.[70]

There have been two impediments to the effective implementation of the EU Treaty. The first is the different views between countries about what constitutes data and thus where the civil liberties boundaries lie. Second are concerns about where lines can be drawn between law enforcement activity and national security.

The Cyber Security Treaty proposed in this paper must address the concept of probable cause which underpins the right of police in a democracy to take action against its citizens when trying to solve a crime. Under probable cause, evidence that is obtained improperly cannot be used. However, there needs to be a very clear distinction between probable cause, law enforcement and legal action taken to prosecute a crime on the one hand and actions taken by intelligence and defense communities to protect a nation's security on the other.

As part of this effort to bring order into the chaos of cyberspace, legal indemnity would cover not just actions taken by law enforcement but also any national security activity. What government, in all its different forms, chooses to do with software and hardware it has purchased is up to government and should not be considered the legal responsibility of the businesses which supplied the goods and services.

The government has already demonstrated that it can work with industry to remove barriers to entry. After the 9/11 terrorist attacks, Congress passed the SAFETY Act in 2002 which provided protections from certain liabilities for suppliers of products, services and software with an anti-terrorist application. For example, in certain circumstances, the SAFETY Act caps the potential liability faced by a company providing anti-terrorism technology. In other circumstances, the Act may provide a complete shield against liability. The SAFETY Act is not designed to directly address conflict in cyberspace, the basic goals of the Act – removing barriers preventing private companies from providing support to the government's cyber defense – can and should be applied to the consequences of collateral damage from the use of software solutions supplied by the private sector to the U.S. government. For example, the current version of the SAFETY Act would not protect a contractor who might be held liable for violating state privacy laws or computer security laws while acting on behalf of state or federal government agencies. It is reasonable to expect that, just as in the terrorism arena, if contractors are going to do their best for the government in supplying the goods and services the government requires, they should be protected from any subsequent legal action that might result.

Thus, the government's first step should be to clarify existing federal law to make clear that support of our country's national security efforts will not be considered criminal. Further, Congress may be able to pre-empt state law in this narrow arena. The federal government should also indemnify contractors providing support for cyber security efforts for damages caused to third parties through the government's use of those products and services. This can be done either contractually or through legislation.

However, even if a new version of the SAFETY Act is passed to cover the cyber realm, the legal environment both within the U.S. and between the U.S. and other countries will remain very confusing. For example, California's Senate Bill 1386 mandates that all businesses, no matter where they are based or where they process information, must take 'adequate measures' to protect personal information of California residents. At the same time, a number of states are trying to protect their citizens against spyware, while the law at the federal level remains unclear and is largely based on previous legislation that was not designed to deal with cyber challenges. At the federal level, Sarbanes Oxley, HIPAA and the Telecommunications Act of 1996 were all designed to deal with non-cyber security issues and yet each affects how data is stored, managed and transmitted.

What this suggests is that a more holistic approach to the legal challenges of conflict in cyberspace is essential on a national and international basis and between government and the private sector. Clarifying these relationships will help leverage the full technological resources that the private sector has to offer.

Law Enforcement

Law enforcement is always going to struggle to police cyberspace effectively. Currently, only 1.5% of FBI agents are trained in solving computer crimes.[71] As a practical matter, this means that for the foreseeable future, the FBI will have to rely on both other government agencies and the private sector for the implementation of a successful policing and prosecution strategy for cyber crimes.

The private sector is frequently the nation's first line of defense. Typically, destructive malware (virus, Trojans, worms, etc.) are tried 'in the wild' before being used against government networks. As a result, private security companies frequently pass data to the government about potential future threats.

However, there is a difference between the detection of a threat and the reporting of an actual attack. While information sharing within an industry has evolved through the creation of a number of Information Sharing and Analysis Centers relating to different industries such as banking and IT, the full potential of the environment has never been realized.

From the outset, industry has been fearful of sharing information with the government for two reasons. First, there is concern that information about an attack that exposes a company's vulnerability and potentially significant financial losses would have a serious effect on stock prices and perhaps create legal exposure. Second, whatever guarantees of confidentiality the government may provide, the private sector fears that the Freedom of Information Act would ensure the release of company confidential information eventually. An effective strategy must consider creating a confidentiality guarantee to protect information shared by the private sector with the government.

Strategic Human Capital

Human capital is the single most vulnerable point in any information technology architecture. At least 80 percent of all attacks are carried out by individuals who are already inside the network and are trusted with passwords and access.[72] Some of these trusted insiders are merely incompetent and careless, while others use their position of trust to provide information to outsiders or to insert malicious code on their behalf. Worse yet, they just steal the data and walk out the door and sell or provide the data to competitors or the highest bidders.

While some software security processes are designed to improve education and training, none have the power of enforcement and almost all are seen as a "box ticking" exercise of little value or significance to most employees.

Education and training are not just intra-organization challenges, they are also necessary for the individual, the organization, the sector and the nation. If the nation knew the degree to which U.S. intellectual property is being stolen, the rate at which cyber attacks are successful, the degree to which vulnerabilities are exploited, and the consequences for the country, there would be pressure for action. This suggests the need for a much higher degree of transparency between the government and the private sector to create a broader understanding of risk and mitigation.

That in turn could create the understanding of the need to educate a new generation of academics, engineers and technical experts that will provide a deep bench of expertise in the U.S. rather than seeing that expertise be outsourced offshore. A broad cyber education program, modeled after the National Cancer Institute's education program, could provide the academic direction and provide funding for professors, doctoral students and associated research teams to tackle these hard issues.

Moving the Agenda Forward

This strategy paper recommends a number of specific components for an effective cyber defense strategy. However, for the strategy to be implemented successfully, further work needs to be done to better understand the practical application of some of the strategic components. Among subjects for further research are:

1) **Trusted Innovation.** The Trusted Foundry and the DARPA Trust in IC's projects are useful starting points for creating a disciplined process to introduce safe technology solutions into the government. How can this process be broadened and deepened to allow for the rapid introduction of both hardware and software from a broad range of suppliers so that government agencies can keep pace with changing technology?

2) **Virtual Vault.** The concept of a Trusted Third Party holding the software codes creates security challenges in its own right. Just how would this work and how could manufacturers and consumers be persuaded to trust the results?

3) **Internet Architecture.** It is agreed that the current structure of the World Wide Web is unstable and chaotic. How practical is a clean sheet solution and if not that, then what?

4) **Leadership.** In both the government and the private sector, effective leadership to create cyber security has proved elusive. How can a leadership approach be applied in government and how can it engage the private sector successfully? How will this approach function more effectively and what would the relationship look like with the private sector?

5) **Civil Liberties and Privacy.** To manage cyber security, the government has a need to know new information that has the potential to infringe on civil liberties and invade privacy. There is a balance to be struck between what industry and individuals must protect and what the government needs to know to manage the nation's cyber security. Where does that balance lie and how can it be legally controlled?

6) **Predictive Analysis.** A layered defense against cyber attack provides one set of defenses but still leaves the initiative with the attacker. A goal should be to deliver predictive analysis to allow a defender some knowledge of where, when and how attacks might appear. This would allow for a proactive defense network. But how might this be achieved?

7) **Cyber Security Treaty.** With the Outer Space Treaty as a possible working model, what are the components of a treaty that would make it effective and how would governments be persuaded to sign and ratify?

8) **Deterrence.** Some argue that deterrence in cyberspace is impossible, while others suggest that it is little different from the process involved in nuclear deterrence. What would the components of a Deterrent Strategy look like and how would it work operationally?

9) **Liability and Indemnification.** Private sector firms continue to face significant risk when building technology and providing services to serve the public when such services create the potential for significant losses due to law suits. How can the Safety Act in the U.S. be used as a model to expand protection to commercial firms in this market throughout the globe?

10) **Federal Organizational Leadership to Include Congressional Oversight.** The cyber world is a network phenomenon requiring different skills from leaders and managers and different organizational structures. What organizational structures can help address the networked problems of the cyber world?

Successive U.S. presidential administrations have recognized the need to defend our cyber infrastructure. However, all measures suggest that the number of successful attacks continues to rise rapidly and the tools employed become more sophisticated every day. These attacks involve organized crime, terrorist groups, nation states, and a multi-billion dollar underground economy that has emerged to exploit the vulnerabilities that exist in every network that operates on the World Wide Web. There is even a large underground economy that sells attack tools to organized criminal gangs and foreign governments to use to attack the United States and its allies, to undermine defense, and steal valuable intellectual property. [73] Action must be taken now to improve the efficiency, security and resiliency of the global cyber infrastructure.

Glossary

Computer Network Attack (CNA) - (DOD) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack. CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.[74]

Electronic Attack - That division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes:

1. Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception; and
2. Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).[75]

Information Operations (IO) - Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Offensive Information Operations - The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to influence adversary decision makers to achieve or promote specific objectives.

Defensive Information Operations - Integrates and coordinates policies and procedures, operations, personnel, and technology to protect and defend information systems. Defensive IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information systems for their own purposes.

Information Assurance (IA) - Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Warfare (IW) - Information Operations conducted during times of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Information - The meaning that a human assigns to data by means of the known conventions used in their representation. It is facts, data, or instructions in any medium or form.

Data - A representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretations, or processing by humans or by automatic means. It is any representation such as characters or analog quantities to which meaning is, or might be, assigned.

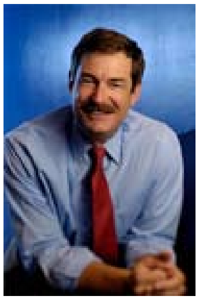
About the Authors

W. Scott Gould

Vice President, Public Sector Strategy and Growth
IBM Global Business Services

Scott Gould directs strategy formulation for IBM's homeland security, intelligence and federal civilian line of business. Previously, he was CEO of The O'Gara Company providing strategic advisory and investment services in the homeland security market. A Naval Intelligence reservist, CAPT Gould was recalled to active duty for Operation Noble Eagle and Enduring Freedom where he served as Deputy to the Director, Naval Criminal Investigative Service (NCIS). He has served as the CFO and Assistant Secretary for Administration at the U.S. Department of Commerce and as Deputy Assistant Secretary for Finance and Management at the Treasury Department. As a 1993-94 White House Fellow, Gould served in the Export-Import Bank of the United States and in the Office of the White House Chief of Staff. Gould is a fellow of the National Academy of Public Administration and a former member of the National Security Agency (NSA) Technical Advisory Group.

Dr. Gould has participated as a panel member on homeland security issues for the Council on Foreign Relations and the Center for Strategic and International Studies as well as a guest lecturer at Harvard University. He is a former member of the Malcolm Baldrige National Quality Award Board of Overseers. He is coauthor of two editions of a monograph entitled: The Homeland Security Market: Corporate and Investment Strategies for the Domestic War on Terrorism as well as Global Movement Management: Securing the Global Economy and Global Movement Management 2.0: Commerce, Security and Resilience in a Networked World and From Vision to Reality: Aligning Business and Government Interests in Maritime Domain Awareness and Global Movement Management.   He is coauthor of a forthcoming book from the Brookings Institution entitled The People Factor: Strengthening America by Investing in the Public Servicer. He holds an AB degree from Cornell University and MBA and Ed.D. degrees from the University of Rochester.



Peter G. Allor
Global Technology Services
Program Manager Intelligence & Vendor Relations, Internet Security Systems (ISS)

Peter Allor is responsible for guiding IBM's overall security intelligence initiatives and participation in enterprise and government implementation strategies.
He is the Vulnerability Coordinator for the IBM ISS X-Force to all vendors and researchers and is responsible for managing X-Force operations where members report vulnerabilities, solutions, best security practices and track Internet attackers globally. Allor is the IBM Board member for the Information Technology - Information Sharing and Analysis Center (IT-ISAC); a member of the Information Technology – Sector Coordinating Council (IT-SCC) Executive Committee; a member of the Forum for Incident Response and Security Teams (FIRST) Steering Committee; and a member of the CSIS Cyber Security Commission for the 44th President. Allor has spoken at numerous events on security, information sharing and cyber intelligence, including Homeland Security for Networked Industries, GFIRST National Conference, FIRST, Infragard National Conference, Forbes Corporate Security Forum, iSecuTech Taiwan and Secret Service San Francisco. In 2005, Allor was presented with IT* Security Magazine's Individual Innovation Award.

Prior to joining ISS, Allor served in the United States Army where he worked in a variety of security related positions reporting from Panama to Korea, as well as the Middle East. Allor holds a bachelor's degree in business administration from Rollins College and a master's degree in organizational management from the University of Phoenix. He is a graduate of the U.S. Army Command and General Staff College.

About IBM's Global Leadership Initiative

IBM's Global Leadership Initiative (GLI) is a lead innovator for Global Business Services clients. GLI identifies critical public sector challenges, convenes expertise from a variety of sources and develops thought leadership to address these challenges. These challenges span a broad range of issue domains including: security, governance, demographics, health care, human capital, economy, environment, education and energy.

GLI consists of former public sector executives, CEOs and leading academics who develop strategic thinking, relationships and opportunities to solve complex problems in the public sector. GLI partners with leading universities, international organizations, think tanks, and other public and private sector institutions in pursuit of its mission.

GLI supports the vision of IBM's Global Business Services for the public sector and works collaboratively with the GBS Industry Team and other IBM lines of business to anticipate and serve client needs.

About IBM Internet Security Systems

IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers. An established leader in security since 1994, ISS' integrated security platform automatically protects against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. ISS products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. ISS' product line is also complemented by comprehensive Managed Security Services. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

Sources

1 http://www.govexec.com/dailyfed/0108/012908j1.htm.

2 "Experts find fault with cyberdirective; Intelligence monitoring authorization reverses 20 years of policy and laws, critics contend", Jason Miller, Federal Computer Week, February 18, 2008.

3 http://encyclopedia.thefreedictionary.com/cyber-.

4 Lt. Gen. Bob Elder, Air Force Cyber Operations Command, Mission: Warfighting, Briefing, January 5, 2007.

5 http://www.dtic.mil/doctrine/jel/doddict/data/c/01182.html.

6 http://www.dtic.mil/doctrine/jel/doddict/data/c/01183.html.

7 http://www.iwar.org.uk/iwar/resources/wikipedia/information-warfare.htm.

8 http://www.acq.osd.mil/dsb/reports/protecting.pdf, p. ES-2.

9 http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

10 The National Strategy to Secure Cyberspace,
The White House, Washington D.C., February 2003. p. viii.

11 Ibid. p.x.

12 http://govexec.com/story_page.cfm?articleid=39466&sid=1.

13 http://www2.csoonline.com/exclusives/column.html?CID=33496.

14 http://online.wsj.com/article_email/SB120147963641320851-
lMyQjAxMDI4MDIxODQyNzg5Wj.html.

15 http://www.govexec.com/story_page.cfm?articleid=38667.

16 http://online.wsj.com/article_email/SB120147963641320851-
lMyQjAxMDI4MDIxODQyNzg5Wj.html.

17 http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece.

18 http://www.mcafee.com/us/research/criminology_report/default.html.
These include: Russia, Israel, France, China, Iran, and Germany

19 http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

20 http://www.isalliance.org/content/view/44/130/.

21 http://business.timesonline.co.uk/tol/business/industry_sectors/technology/
article2980250.ece.

22 http://www.nytimes.com/2007/05/29/technology/29estonia.html ; Rebecca Grant, Victory in Cyberspace, Air Force Association, October 2007, pp.4-9.

23 http://www.networkworld.com/community/node/30970; http://www.circleid.com/posts
russian_cyber_attack_on_georgia/; http://georgiamfa.blogspot.com/2008/08/cyber
attacks-disable-georgian-websites.html

24 The U.S. government is not a standards body and any standard set by the public sector must be done collaboratively with the private sector, especially because an imposed U.S. standard will be followed by other countries and could risk putting U.S. companies at a serious competitive disadvantage.

25 http://www.acq.osd.mil/dsb/reports/protecting.pdf p.ES-2.

26 http://en.wikipedia.org/wiki/Moonlight_Maze; http://www.sfgate.com/cgi-bin/article.cgi?file=
chronicle/archive/1999/10/07/MN58558.DTL&type=tech_article.

[27] http://en.wikipedia.org/wiki/Titan_Rain; http://www.time.com/time/magazine/article/0,9171,1098961,00.html.

[28] http://en.wikipedia.org/wiki/Cyber-terrorism ; http://www.usatoday.comtechnews/2002/01/28/security-study.htm;http://news.zdnet.co.uksecurity/0,1000000189,3921200-2,00.htm; Jones, David Martin Globalization and the New Terror: The Asia Pacific Dimension, Edward Elgar Publishing, Cheltenham (UK), 2004, p.153.

[29] Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.

[30] http://www-03.ibm.com/press/us/en/pressrelease/19141.wss

[31] http://www.engineeringchallenges.org/cms/8996/9042.aspx.

[32] There is some contention, however, around the longevity of Moore's law. Bernie Meyerson (IBM Fellow, VP Strategic Alliances and Chief Technologist), who leads IBM's semiconductor R&D, posits that Moore's Law is no longer guaranteed. Moore himself has noted that future progress will be difficult and likely to some degree slower. Chips now require vast amounts of electricity, a growing portion of which is dissipated through leakage. Designers are going to have to add technologies such as strained silicon to their chips and to redesign transistors to control energy consumption. For further information see: http://news.cnet.com/2100-1001-984051.html?hhTest=1.

[33] http://www.csis.org/media/csis/pubs/070323_lewisforeigninflubook.pdf p. 17.

[34] http://www.atimes.com/atimes/South_Asia/HA28Df01.html.

[35] Popular Mechanics, April 2008.

[36] http://www.sei.cmu.edu/cmmi/models/.

[37] http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002.

[38] Revitalizing Federal Cyber security, Sans Institute, December 12, 2006, p.2.

[39] http://www.govexec.com/dailyfed/0407/042007p1.htm.

[40] ibid.

[41] http://www.govexec.com/story_page.cfm?articleid=39314&dcn=e_gvet.

[42] According to the law, "Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. Each evaluation under this section shall include: (a) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; (b) an assessment (made on the basis of the results of the testing) of compliance with the requirements of this subchapter; and related information security policies, procedures, standards, and guidelines; and (c) Separate presentations, as appropriate, regarding information security relating to national security systems." In regards to independent auditors, the law states (a) "for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency;" and (b) "for agencies that do not have Inspectors General, the head of the agency shall engage an independent external auditor to perform the evaluation."

[43] Interview with John Lainhart dated February 19, 2008.

[44] http://www.gcn.com/online/vol1_no1/45563-1.html?topic=FISMA.

[45] http://articles.latimes.com/2002/nov/25/business/fi-portecon25.

[46] http://www-935.ibm.com/services/us/gbs/bus/pdf/global-movement-management-exec-summary.pdf.

[47] http://www.govexec.com/dailyfed/0208/022208bb1.html.

[48] http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf, p. 11.

[49] http://taosecurity.blogspot.com/2007/12/feds-plan-to-reduce-then-monitor.html; http://www.securityfocus.com/news/11507.

[50] http://en.wikipedia.org/wiki/US_intelligence_community_A-Space.

[51] http://www.afei.org/documents/HonorableJohnG.pdf, p. 2.

[52] Ibid.

[53] Ibid.

[54] http://en.wikipedia.org/wiki/US_intelligence_community_A-Space.

[55] Revitalizing Federal Cyber security, Sans Institute, December 12, 2006, p. 4.

[56] http://www.msnbc.msn.com/id/13819339.

[57] http://www.businessofgovernment.org/pdfs/GMM.pdf.

[58] http://www.globalsecurity.org/military/library/news/2007/09/mil-070927-afps06.htm.

[59] http://www.umsl.edu/~keelr/200/ratchoc.html.

[60] http://www.securityaffairs.org/issues/2006/10/cilluffo_nicholas.php.

[61] http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp.

[62] http://www.gcn.com/online/vol1_no1/43089-1.html.

[63] http://en.wikipedia.org/wiki/Outer_Space_Treaty.

[64] Statement of Lt.Gen. William Campbell, DISC4, Hearing on Information Assurance and Information Superiority, http://www.globalsecurity.org/intell/library/congress/2000_hr/0003-08campbell.htm.

[65] http://www.cyberconflict.org/pdf/WingfieldPresentation.pdf.

[66] http://www.crime-research.org/library/White.htm.

[67] In addition to the legal concerns, the foreign country could take retaliatory action against the company's overseas subsidiaries.

[68] http://news.zdnet.co.uk/itmanagement/0,1000000308,39149470,00.htm

[69] http://www.euractiv.com/en/infosociety/international-treaty-cybercrime-moves-closer article-115837

[70] http://news.zdnet.co.uk/security/0,1000000189,39166977,00.htm

[71] http://www.independent.org/newsroom/article.asp?id=1063.

[72] http://www.gsnmagazine.com/cms/features/columns/202.html; http://www.bizforum org/whitepapers/rand001.htm.

[73] http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminologyReport07.pdf.

[74] http://www.iwar.org.uk/iwar/index.htm.

[75] http://www.au.af.mil/info-ops/what.htm.

IBM Global Business Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
10-08
All Rights Reserved