Cyber Security for the Department of Defense

Paul A. Strassmann

Distinguished Professor of Information Sciences, George Mason University

Former Director of Defense Information, Office of the Secretary of Defense

June 30, 2009

DRAFT COPY

Abstract

This paper concentrates on safeguarding the information security of DOD. It addresses issues such as the reasons for the creation of the USCYBERCOM; the affordability of cyber defense technologies; the achievement of acceptable levels of security and what changes in the organization of information assurance are necessary.

A case is made for implementing uninterrupted surveillance of every one of the millions of connections to the Global Information Grid. Emphasis is placed on the achievement of manpower cost reductions to fund the migration from 15,000 networks to a much smaller number that can be managed and controlled from Network Operations Centers. The security defects of the Internet are noted and countermeasures are recommended. The archiving of all transactions becomes necessary as a way of countering insider threats.

The creation of the USCYBERCOM is compared with the challenges of creating the technology and acquiring the manpower resources to make nuclear submarines feasible in the 1950's. Cyber security for DOD will be attained when everyone includes it as a component of all warfare.

Cyber Security for the Department of Defense

On June 15, 2009, Deputy Secretary of Defense William J. Lynn addressed the Center for Strategic and International Studies on: "Protecting the Domain: Cyber security as a Defense Priority." Lynn said, "…in DOD there are an estimated 90,000 personnel engaged in administering, monitoring and defending 15,000 networks connecting seven million computers. If attacked in milliseconds, we can't take days to organize and coordinate our defenses. If our networks were to be disrupted or damaged, we'd need to respond rapidly at network speed before the networks could become compromised and ongoing operations and the lives of our military are threatened. In short, we have to be just as fast, if not faster, than those who would do us harm."[1] Lynn proposed to increase the size of FY10 cyber security funding to add more cyber experts.[2]

With the huge numbers of intrusions an excessive number of networks cannot be defended economically. DOD must operate with a vastly smaller number of networks. Reliance primarily on added operators is insufficient. DOD networks should have as the primary line of defense automated cyber security diagnostics that have instant response times.[3] Such software is now commercially available and has been already applied widely.

There is no question that cyber security has now become the top priority for all IT planning. It affects each of the 7,166 major information systems programs in FY10.[4] These programs are interconnected in ways that makes every network and each of the seven million computers potentially an entry point for hostile invasion.

Cyber Security as a Defense Priority

To implement cyber security, Secretary of Defense, Robert M. Gates announced on June 23, 2009 the U.S. Cyber Command (USCYBERCOM), which will assume the responsibility for defending the military cyberspace.[5] With the dissolution of the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW) the USCYBERCOM takes over, as a unified command, the operations of the Army, Navy and Air Force networks. How that will be accomplished will be directed by the USCYBERCOM and will be submitted through USSTRACOM to the Joint Staff as well as to the Office of the Undersecretary of Defense (Policy).

The most significant change in policy is the re-designation of the position of the Director, of the National Security Agency (DIRNSA) as also the Commander of USCYBERCOM. This brings both organizations with cyber security expertise under a unified military command. The purpose of the combination of USCYBERCOM and NSA is to deliver to DOD a well-protected information infrastructure.[6]

The purpose of this paper is to outline the scope of what USCYBERCOM will have to accomplish. The issues are: Why is USCYBERCOM necessary? What affordable technologies are required? How to achieve an acceptable level of security? What is the urgency of cyber defenses? What changes in governance are necessary?

Why is USCYBERCOM Necessary?

The major obstacle in adopting cyber security is the military culture that views kinetic warfare (rifles, cannons, bombs) as the primarily means for waging wars. Warfare is now changing. Electronics now precedes kinetics:

- Kinetic weapons are deployed rarely. Information warfare is uninterrupted.
- A large logistic tail supports every kinetic attack. It takes only a handful of hackers to launch cyber attacks.
- Warfare behind enemy lines used to be rare. In cyber wars thousands of computers can be captured in any location.
- Kinetic attacks take minutes or hours, with the warriors idle most of the time. In cyber wars actions are executed in microseconds, with attackers working continuously.
- When kinetic attacks fail the attacker loses. When cyber attacks fail the attacker wins because he has collected intelligence.

The question whether cyber attacks are an act of war is still being debated. Regardless of that cyber security must be fused with conventional warfare. Everyone – not only a selected class of cyber war specialists – is now engaged in cyber warfare. The transfer of the responsibility for network assurance from the Armed Forces and Agencies to the USCYBERCOM is a necessity. The consolidation of cyber security under a single unified command is required to overcome the organizational disconnects that currently prevail in DOD.

What Technologies Are Needed?

Uninterrupted surveillance is mandatory for all cyber security because information attacks can be executed instantly. Protection can be obtained only by means of automated real-time surveillance. Humans are too slow and excessively error prone to cope with the onslaught of thousands of attempted intrusions. Operator responses cannot cope with the changing complexity of incoming signals whenever an attack is taking place.

When systems are breached, the defenders must discover what happens by examining incoming transactions through layers of software and hardware filters. Sorting out already known viruses accounts for only a small part of what needs to be examined. The attackers may fail in attempts to corrupt networks but can also easily re-target attacks in seconds. Instant reactions by the defenders are essential because it is easy for a cyber-attacker to disappear whenever detected, only to re-appear in a different disguise a moment later. Cyber security defenders must manage protection without any downtime whatsoever because the aggressors can check out the targets without a pause. The attackers will be looking for brief lapses in monitoring to find opportunities for sneaking in a bogus code into the defender's computers.

The demanding requirements for quick and uninterrupted responses are necessary because every compromised system can disgorge huge amounts of data to the enemy unless a suspected incursion is

instantly cut off.[7] Even more serious is the injection of small amounts of "malware" code that places "back doors" for uncontrolled access that will cause a system to crash at critical times. The attacker's options to corrupt systems are unlimited. Groups of experts refine attack scenarios and share network penetration techniques.

The menu of attack methods is very large, such as: "denials of service"; "saturation attacks"; "exploit tools"; "logic bombs"; "sniffers"; "Trojan Horses" and "worms". Many of these methods are aimed not only at thousands of servers but also at millions of personal computers, especially those that are controlled by Microsoft software. Installation of hardware firewalls or anti-virus software will lessen the damage provided that the defenders' software has been properly updated and everybody follows security rules. Unfortunately, this works only in cases where the "signature" of an incoming attack is known beforehand.

Aggressive countermeasures must protect against conditions that are not trapped otherwise. This must include dealing with "zero day" defects, which are virus attacks for which there is no known identification template against which firewalls or anti-virus software could apply protective measures. Under condition of cyber warfare one must always assume that intrusions will be executed as "zero day" attacks.

Network disabling attacks, which qualify as "information warfare", cannot be deflected solely by firewalls or anti-virus measures located in servers or personal computers. The adversary will also try to attack servers, routers and switches that are intermediaries in connecting circuits as a message "hops" from one connection to another. In the Internet it make take anywhere from five to fifteen "hops" for a message to get from origin to destination.[8]

Unless DOD communications take advantage of rarely used point-to-point connections, almost every transmission takes place by means of the Internet communication protocol. The problem is that Internet is insecure. The most dangerous method for disabling networks is to insert somewhere in the communication links "spy ware" (software that surreptitiously tracks or transmits data to a third party) or, "botnets" (software robots that allow an unauthorized user to control compromised servers). The inherent insecurity of Internet and of inevitable human lapses by the network defenders makes that possible.

Network-disabling attack software can be purchased from on-line sources as "training aids." Such purchases are not traceable because they use anonymous email links.[9] For more sophisticated disruptive assignments there are also cyber-mercenaries who will penetrate designated targets for a fee. The current diplomatic negotiations about preventing cyber attacks by means of a treaty are irrelevant from a DOD standpoint. Any cyber strike against military targets can be disguised as assaults performed by unauthorized non-state agents.

It will be necessary to make large investments in cyber security software to inhibit almost all cyber attacks. Proceeding with the current approach of spending money on diverse and uncoordinated information assurance projects that protect too many networks is neither affordable nor executable with the resources we have available. It would be one of the primary objectives of USCYBERCOM to acquire cyber defense capabilities as highly classified assets. DOD will not be able to rely on commercial security sources for its protection. The close association between USCYBERCOM and the National Security Agency (NSA) offers a talent pool of expertise that will be capable of delivering to DOD software that will intercept almost all attacks.

Thin Clients

Firewalls and antivirus software installed individually on every desktop often causes more problems than rogue codes.[10] Server and workstation performance can slow down to a crawl because complex software is stacked up in many added layers on top defect-prone operating systems. End user service performance will degrade. Administrators will spend countless hours troubleshooting problems and reconfiguring antivirus software while installing numerous software "patches" that are generated every time a vendor discovers a new vulnerability.

The remedy to hard to manage software, which resides on each of the millions of computer devices, is to relocate the security functions to a much smaller number of servers performing what is now defined as "cloud computing".[11] Network Control Centers (NOCs) are then in a better position to control individual servers, which in turn can service over 2,000 personal computers with a single set of cyber-resistant software.[12] The cost savings in hardware, software and administrative personnel could be as high as 50 percent.

Network Control Centers – Cyber Security Defenses

Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any countermeasures. Their objective is to launch probes that will support the planning how to penetrate defenses from multiple points of entry. Many of these probes, injected in stealth, are to construct detailed maps of the defender's circuits, switches, routers, servers and workstations and not to cause any disruption. Active attacks are only one of many possible results. Discrediting communications or faking the authenticity of messages is one of the many ways in which damage can be inflicted.

The means for enforcing compliance with the security policies and security standards is the fielding of NOCs.[13] NOCs maintain real-time awareness of the condition of every one of the current seven million Internet Protocol (IP) addresses in DOD. This number will grow to hundreds of millions when DOD adopts Radio Frequency tags for its logistics pipeline.

Any one NOC monitoring position can cover well over a million IP's. Therefore, NOC operations will be geographically distributed and must be redundant to assure continuity of operations. The NOCs will always be a target of cyber attacks under any information warfare scenario. It will require at least three NOCs to have the capacity to manage any one regional network. The GIG will have to depend on assured fallback of any computing node, regardless where a failure may occur in any parts of the network.

Figure 1 - Example of a Network Operations Center[14]

The DOD NOCs, while retaining configuration oversight over hardware and software of the entire network, may have to delegate parts of the surveillance to subordinate support centers, such as offered by secure network vendors. Vendor-operated NOCs, but under complete control from USCYBERCOM, can be then used for monitoring local circuit conditions. However, the USCYBERCOM will always remain responsible for handling every incident that is detected as a possible information compromise.

Investments in the automated detection of suspected cyber attacks will allow for a substantial reduction in the personnel to staff the NOCs. The NOC operations will not, however, provide assurance that every adversary action will completely escape detection. That is why the cyber security design must provide for additional layers of defenses that include human operators who can concentrate on intercepts that have been already identified by means of automated means as of suspicious origin.

NOCs must always monitor how data is transferred between internal and external communication links. This includes communications from the Global Information Grid (GIG) to contractors or suppliers and vice versa. Monitoring must also keep track of every Wide Area Network (WAN) and Local Area Network (LAN) to assure that all communication transactions can be traced from origin to their destination.

The NOCs must be able to re-route traffic under conditions of failure or whenever a potential attack is detected. Spare circuits must be available to divert communications to more secure sites. Network management will have keep track of every electronic asset as it connects or disconnects from the GIG. One of the uses of such an inventory will be to identify alternative communication paths under condition of failure as well as to discover attempts by rogue operators to plant unauthorized devices on the GIG.

The most important function of the NOC is to account for every Internet Protocol (IP) address, which includes all desktops, laptops, personal digital assistants (PDAs), cell phones and RFID (Radio-frequency Identification) tags. This includes router and switch IPs, which account for the location, function and capacity of these devices. Routers and switches perform network functions such as the reassembly of packets and the reporting of errors. They become targets by which information warfare

attackers can seek to disguise their access to the GIG. This is possible because routers and switches are maintained by remotely managed vendor diagnostics. The vendor's access security may not be good enough to meet GIG requirements.

How to Achieve Acceptable Levels of Cyber Security?

We must reconcile ourselves with the fact that Internet is fundamentally an insecure (and toxic) communication medium. Its protocols have been designed to support academics whose objectives were to achieve easy exchanges of information. The original design of Internet is still in place and remains embedded in DOD networks that use Internet connections.

Vinton Cerf, the co-designer of Internet, recently said that anyone who performs transactions over the Internet should worry about the security of this technology. According to Cerf one of the most critical needs is authentication because Internet does not make automatically available end-to-end verification of transaction deliveries. Putting into place encrypted "tunnels" is insufficient because that does not confirm the identity of the endpoints of a transaction. For instance, one can have email with an attached virus. It can be encrypted and then sent through encrypted communication links. Once it gets to the other end, the transmission gets decrypted. The virus can then become toxic. This lack of authentication is particularly acute when trying to secure mobile communications, which in the future will exceed landline transmissions.[15]

Researchers have proposed ways how to remedy the insecurity of Internet, though implementation that may be at least a decade away.[16] Given the lack of verifiable Internet authentication, DOD must meanwhile rely on sender as well as recipient identification to attain cyber security.

Managing Access Privileges

Securing access privileges to the defense networks will have to depend on the strict enforcement of access authorizations. Improved versions of the Common Access Cards (CAC) must be mandatory for all communications. Unauthorized entries will have to be managed so that security privileges can be revoked in seconds as anomalies are detected. This will require instant tracking of any changes in the status of personnel, including of coalition partners and contractors.

Real-time management of CAC will require the installation of procedures to assure that there is no time gap while an information attacker can masquerade as a legitimate CAC holder. The database containing CAC authorizations should be able to alter CAC identifying codes whenever there are questions about their authenticity. CAC cards now include Public Key Infrastructure (PKI) identification but that may not be sufficient to automatically grant access privileges. For cyber security the NOCs must be able to compartmentalize network access depending on mission, location or functions performed. CAC cards must be further augmented to include biometrics for accesses that require special protection. The defense networks must offer one-time access privileges to network partners for a limited time or for a restricted purpose.

The networks must also offer ports to all DOD personnel for unencrypted access to the public Internet for social or personal uses. DOD can deliver such service through a variety of means provided that such links remain under the control of the NOCs and remain completely isolated from the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) or the Secret Internet Protocol

Router Network (SIPRNET). Nevertheless, all social or personal communications on the GIG as well as all DOD official traffic will have to be logged into archival databases for retention in perpetuity.[17]

Insider Threats

Rogue employees, consultants or contractors are sources of insider cyber attacks.[18] Such risks are exacerbated by the grant of access to systems and databases by authorized parties.[19] Though insider compromises will be always fewer in the number incidents, the resulting damage will be always much larger. In cases of internal breaches one must always assume the possibility of collusions taking place. Therefore, each suspicious network incident will have to be followed up and documented for a further examination as to probable patterns of malfeasance.[20] The risks inherent to the GIG, which connects with a multiplicity of external networks, arise from instances when any one of the trusted business partners becomes a conduit for third party attacks. Unusual amounts of suspected traffic with external networks may indicate that an invasion may be taking place.

Countermeasures

All security is imperfect since no technology can assure 100 percent protection. Cyber security must be achieved by pursuing a layered approach where a combination of partially reliable measures can deliver a statistically improved probability of security, which cannot be offered by reliance on any one defensive method.[21] After all of the automated protection measures are applied, the innermost layer of defense will always have to depend on human intelligence.

Countermeasures will have to be constructed to discover anomalies that are not intercepted by software. Special purpose traps will have to be built to capture traffic from suspected sources.[22] This is an arena where the most imaginative and innovative personnel would have to be employed. Their qualifications would be similar to that required by counter-intelligence or NSA officers possessing skills how to deal with the highly technical aspects of electronic communications. Such personnel will assume positions that will require long-term tenure. That is necessary for the preservation of specialized expertise.

The primary source of data how to deal with information attacks is the transaction archives, which retain in perpetuity every single access to the GIG. Software, such as artificial intelligence, forensic methods and pattern recognition methods will enhance the brainpower of the cyber experts to discover inconsistencies in any transmission.

What is the Urgency of Cyber Security?

The DOD information technology spending for information security is $2.9 billion, or 8.5 percent of total IT spending.[23] On top of that we have communication spending that is $10.7 billion, or 31.3 percent of total IT spending. [24] These amounts do not include payroll costs of military and civilian workforce. The communication plus the cyber security infrastructure consumes almost as much money as is allocated to the war fighter missions. This spending is spread over a hundreds of projects that do not share identical data elements and do not use interoperable standards.[25] From a financial standpoint one must therefore view the entire DOD security and communications infrastructure as an overhead cost and not as a direct cost for executing warfare missions. One of the objectives for USCYBERCOM would be to lower the overhead costs incurred in the protection of communications that support warfare.

Most of the cyber security budget is for Agencies ($1.7 billion), with spending for the Army at $346 million, the Navy at $336 million and the Air Force at $522 million. Altogether, the information security budget funds 52 projects, mostly for compliance with "information assurance" requirements of OSD Instructions. These are mostly policy-level documents, which are process rather than execution oriented. The OSD policy guidance does not address how cyber security will be funded and how it can be implemented. There is only one major development project that could be viewed as a major investment in DOD-wide cyber security for $379 million.[26] It accounts for only 1.1 percent of the total DOD IT spending.

These budgets do not suggest that cyber security is a DOD investment priority. The recent increases in information security spending can be seen only as appendages placed on top of the existing 15,000 networks. At present DOD has too many networks and pursues only limited Joint investments for the reduction in enterprise-level network spending. DOD cannot achieve information security in the foreseeable future except if USCYBERCOM will have the authority to redirect Armed Forces and Agencies spending for communications.

DOD Communication Costs - $Millions	Number of Programs	FY'10 Spending
Navy, Marine Corps	30	$1,122
Army	8	$2,510
Air Force	38	$2,989
Agencies	44	$4,033
Total DOD	120	$10,655

Table 1 – DOD Spending for Communication

Most of the communication budget is for Agencies at $4 billion, with spending for the Army at $2.5 billion, the Navy at $1.1 billion and the Air Force at $2.9 billion. Altogether, the communication budget supports 120 programs, many with duplicate circuits that are run to identical locations. A review of each of the 120 programs does not suggest that cost reduction is a DOD priority. The existing networks have grown to satisfy program-driven needs without regard of the costs of cyber security or of shared circuit economics.

What Change in Governance is Necessary?

Cyber security is a DOD Information Enterprise mission. The Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO) is responsible for setting cyber security policies. He directs security through DOD Enterprise Architecture, which provides the standards for delivering such capabilities. This defines the GIG as a "…globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel."[27] The purpose of the GIG is to encompass all DOD communications, computing services,

software, applications and data that can be defined as Joint "enterprise services". This is an enormous charter that cannot be executed as a coherent Information Enterprise mission. This is why the SECDEF has correctly concentrated on securing the GIG as the immediate priority.

The USCYBERCOM implementation plan will be transmitted through USSTRATCOM to the Joint Chiefs and to the Office of the Undersecretary of Defense (Policy) and not through the ASD NII/CIO. DISA will be also relieved of managing the Joint Task Force for Global Network Operations (JTF-GNO) to become managed directly by USCYBERCOM. This signals the diminishing roles of the DOD CIO and of DISA as information security becomes the driving influence how networks will be managed through USSTRATCOM, NSA and USCYBERCOM.

The question is how will USCYBERCOM manage cyber security budgets on an enterprise-wide basis? Though DISA operates many of the Defense Enterprise Computing Centers (DECCs) and leases a large share of DOD communications circuits, most of the costs of computing and of telecommunications remain with the Components where they are controlled as a program expense. Through USCYBERCOM DOD will now acquire a unified and consistent approach to network cyber security.[28] What is still missing is clarity as to what share of network assets and budgets will be transferred from the Components to the USCYBERCOM.

Skilled Manpower

The highest immediate priority for cyber security is to acquire expert personnel to manage the GIG as a DOD enterprise operation. That makes it necessary to develop human capital on a scale that is only comparable to the acquisition of a nuclear submarine force in the 1950's. However, implementing cyber security should be now easier because DOD does not need to develop an industrial base for the construction and operation of its networks. Network technologies are readily available now especially in handling secure financial transactions. It is the acquisition of skilled manpower in DOD – and not of technology - that will determine how soon we can expect cyber security to be realized.

Existing Component operations depend on custom-built infrastructures for networks and applications. However, individual programs are driven by program schedule and budget but not by operating costs. Therefore each program pays separately for protection against information warfare attacks. DOD will then spend most of its program costs for communication infrastructures that cannot fund adequate cyber security investments.

One could possibly speculate about prolonging the reliance on the current incompatible environments for another decade. That would offer diffused defenses, which would present smaller targets to attack without incurring most of the conversion costs of networks to the GIG. Such an option is not viable because every network that is inadequately protected can offer an entry point to those parts of DOD that are defended better. That is why the scarcity of funds, the operational risks from rising information attacks and the enormous scope of what needs to be done dictates the merger of the existing networks into a unified GIG that would be managed by USCYBERCOM for the delivery of cyber security as fast as is possible.

Consolidated and fully automated cyber security calls for less manpower but with more capabilities. One of the missions for USCYBERCOM will be to capitalize diagnostic, surveillance and countermeasure methods. A smaller information community will cost less because much of the labor for

monitoring of security risks and for managing information technology assets can be taken over by automated systems. The economics of information and communications technologies favor such a shift. The prices of computing hardware are dropping rapidly while the full costs of personnel are rising. Savings will be available for re-investments in improved network protection in order to keep up with the attackers' steady innovations.

Cyber warfare as the Fourth Branch of the Military?

It has been suggested that the cultures of the Army, Navy and the Air Force are incompatible with that of cyber warfare. The Armed Forces operate in the kinetic arena where the application of physical force is the primary objective. In contrast, cyber warfare exists in the non-kinetic world of information flows, network protocols, and hardware and software vulnerabilities.[29] That is why the creation of fourth branch of the military to conduct cyber warfare was under consideration. How offensive cyber warfare should be organized is different from the ways in which cyber defenses can be implemented. This is why this paper concentrates only on cyber defenses.

Networks that support applications are already embedded in the Armed Forces, with each having unique requirements. The submarine force has different application needs from those supporting the Army Rangers. Business applications in Finance are different from those of Health Care. The National Missile Agency must apply different standards to information assurance than Human Resources.

Cyber security ought to consume less than 10 percent of the IT budgets and therefore must be always seen as an infrastructure function and not as one that dictates warfare requirements. Providing cyber security as a support service will be demanding but not decisive from a fiscal standpoint during the migration of 15,000 networks into the GIG. Most of the IT costs in DOD should be spent for applications that are tightly linked to the needs of individual Armed Forces and which depend on cyber security only as an enabler. If there would be a Cyber Warfare Fourth Branch it would have to delegate to the Armed Forces the responsibility for managing most of the available funds anyway. It remains to be seen how USCYBERCOM will control the cyber security budget to be carved out from the Armed Forces and Agencies.

Summary

Information technologies have progressed sufficiently that they have shifted to a dependency on networks and not on the power of individual computers. That is why USCYBERCOM will have to start with a drastic reduction in the number of separate networks so that cost reductions in operating personnel can be used to fund an accelerated migration to the GIG architecture.

The achievement of cyber security must be seen as the race against network-using attackers who potentially have the capacity to prevent the DOD from engaging in its warfare business. Whenever such damage will take place is only a guess. The cold fact is that the attackers are already in place and are learning fast how to apply cyber warfare as an effective weapon.

[1] Kruzel, J.K., "Cybersecurity Poses Unprecedented Challenge to National Security", U.S. Department of Defense, June 15, 2009, available at http://www.defenselink.mil/news/newsarticle.aspx?id=54787.

[2] Grant, G., "Lynn Wants Halt to Cyber Sniping", *DoD Buzz*, June 16th, 2009

[3] For instance, AKAMAI, a U.S. network management firm, can economically monitor over 1,000 large networks with 20 percent of U.S.A. Internet traffic, controlling more than 48,000 servers with less than 12 operators. For details see http://www.akamai.com/html/technology/index.html.

[4] Federal IT Spending for Budget Year 2010 (May 11, 2009), available at http://www.whitehouse.gov/omb/e-gov/.

[5] The Secretary of Defense, "Establishment of a Subordinated Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations", Letter dated June 23, 2009

[6] How this change will affect relationships between the NSA and the CIA, FBI, foreign intelligence and the Homeland Security Department is yet to be worked out.

[7] A denial of service attack on Internet "root" computers in December 1992 (while the author was CIO of NASA) was contained by cutting off most of the incoming connections to the critical NASA "root" computer.

[8] At each transmission point the electronic pulses must pass through five layers of circuits. In case of an error, the entire process must restart from its origin.

[9] Strassmann, P.A., and Marlow, W., "Risk-Free Access Into The Global Information Infrastructure Via Anonymous Re-Mailers." *Symposium on the Global Information Infrastructure*, Cambridge, MA, January 28-30, 1996 available at http://www.strassmann.com/pubs/anon-remail.html.

[10] "Take a Bite out of Bloatware", *Sunbelt Software*, October 2008, available at http://www.sunbeltsoftware.com.

[11] A description of the technologies that favor the relocation of software functions from desktops and laptops to servers can be viewed in http://www.vmware.com/solutions/datacenter/.

[12] This is known as "virtualization".

[13] Such an approach calls for the concentration of expensive intrusion detection "appliances" in NOCs instead of distributing them to each network. The International Data Corporation estimates that 80 percent of network security functions will be ultimately delivered via security appliances.

[14] The NASA national network operations center at the Marshall Space Flight Center.

[15] Thibodeau, P., "The Internet is incomplete, says its co-designer, Vinton Cerf." *Computerworld* June 11, 2009.

[16] The Digital Object Architecture (DOA) provides a means of identifying and protecting digital information in a network environment. It was developed with support from the Defense Advanced Research Projects Agency (DARPA). For details see http://handle.net/.

[17] DoD 5015.02-STD mandates the archiving of all email as well as computer reports. The stored records will apply "de-duplication" technologies to minimize data storage requirements. The archives are necessary for a historical analysis of communication patterns, which is necessary for discovery of insider compromises.

[18] Deloitte Touche Tohmatsu., "Global Financial Services Industry Security Survey, 2008."

[19] SANS (Systems Administration, Audit, Network, Security) Institute, "Top Ten Cyber Security Menaces for 2008."

[20] There is an estimated 700 NIPRNET email domains inside DOD, handling approximately 50 million messages per day that must be screened. See *Military Information Technology*, June 2009, p.2. Scanning this traffic would require "deep packet inspection" hardware and software, which is not affordable for 700 email domains.

[21] Even a relative high level of 99.999 percent reliability for four layers of cyber defenses will still have a downtime of 21 minutes/year (calculated as 365*24*60*0.00004), which may not be good enough under conditions of information warfare. Downtimes are not normally distributed, but cluster around infrequent incidents. Improved downtimes should be achieved economically through a redundant architecture combined with a complete isolation of mission-critical networks from external sources. The GIG will have to end up as a collection of networks offering different levels of protection.

[22] This requires construction of "honeypots", which are traps set up to detect unauthorized use of information systems.

[23] Office of E-Government & Information Technology, Visualization to Understand Expenditures in Information Technology (VUE-IT), available at http://www.whitehouse.gov/omb/egov/vue-it/index.html#path5/group499LOB404/subLOB140/subLOB140.json. They are FY09 costs.

[24] Office of E-Government & Information Technology, available at http://www.whitehouse.gov/omb/e-gov/. These are FY10 costs.

[25] Deloitte Touche Tohmatsu, *Global Financial Services Industry, Security Survey 2008*. Most of the financial firms spend from 1-3 percent of the IT budget on information security.

[26] Office of E-Government & Information Technology, available at http://www.whitehouse.gov/omb/egov/vue-it/index.html#path5/group499LOB404/subLOB140/agency007/agency007.json

[27] DOD Directive 8000.01, "Management of the Department of Defense Information Enterprise", February 10. 2009

[28] There are 120 major programs in place, managed by separate Program Managers and implemented by a much large number of contractor firms.

[29] Conti, G., Surdu. J., "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?", *IA Newsletter*, Vol 12 No 1, Spring 2009.