Securing DoD Networks for the 21st Century

Dr. Daniel Goure
Lexington Institute

September 2015

Executive Summary

Some forty years ago, the U.S. Armed Forces began a revolution in military affairs based largely on the exploitation of information. A series of advances in position location, accurate munitions guidance, multi-spectral surveillance, data fusion and, most importantly, network connectivity resulted in a new type of military. Success in modern war of any character, scale or intensity, is increasingly a function of how successfully military institutions, insurgents and even terrorist groups are in exploiting, managing, manipulating and countering information networks.

Net-based intelligence and warfare are now being challenged by the exploding field of cyber attack. U.S. adversaries are developing strategies, doctrines, operational art, tactics, techniques, technologies and specialized organizations to conduct cyber espionage and warfare. Given the U.S. military's dependence on networks, an advantage in the area of network attack could be sufficient to give our enemies a true war-winning advantage.

It is no longer permissible to treat cyber security as an afterthought, an applique or even a cost of doing business. The security of the entire defense enterprise against cyber intrusion must be approached with all the seriousness and investment of resources and personnel that the U.S. military devoted to key areas of national preeminence such as nuclear weapons, electronic warfare, undersea warfare and air dominance. There is no value to investing in the best network technologies if they are vulnerable to attack. Success in future conflicts will go to the side best able to defend their networks from penetration, exploitation and attack.

So, how should the Department of Defense (DoD) proceed to create a 21st Century network security system? First, the Department must think and act strategically. The DoD's aggregation of endpoints and networks is changing and expanding with the introduction of new users, devices, capabilities and applications. Such a universe of information nodes can only be managed, directed and, ultimately, protected by a comprehensive security architecture supported and even guided by a single management system. Only with a single security architecture defining standards, rules and procedures can comprehensive security be achieved. Modern end-point security requires a centralized management platform, one that provides end-to-end situational awareness, ensures the implementation of security procedures and and supports the necessary configuration control.

Establishing an appropriate organizational and management structure for DoD's networks is only the first step in the process of achieving comprehensive cyber security. Next there must be a strategy that exploits existing capabilities, enhancing them where possible and introducing new security technologies as needed. Cyber security is the quintessential competitive strategy in which each offensive action produces a corresponding defensive measure which, in turn, propels the offense to renew its search of another avenue of advance. Security must be more pro-active rather than reactive, imposing costs on the attacker and addressing the entire threat life cycle. It must increasingly turn to automation in order to surveil the entire information enterprise, match the threat's agility and respond at network speed.

Finally, a comprehensive strategy for network security must leverage the power, inventiveness and agility of the commercial IT industry. Recognizing the pace of innovation in the private sector, DoD must find an alternative model for the acquisition of cyber security capabilities, one that takes advantage of innovation in the private sector to match the speed of the threat.

Effective and Secure Networks: The Heart of U.S. Military Operations

Military power in the 21st Century will not be denominated according to the traditional units of account, tanks, planes and ships, but in terms of the breadth, sophistication, speed and security of the networks that empower a nation's or group's armed forces. Secure networks are vital to U.S. military operations at all levels and are a source of tactical, operational and strategic advantages. They provide the capability to acquire, move and process massive amounts of information, make decisions rapidly and command distributed forces on an unparalleled scale. Today, the U.S. military is able to utilize the power of its networks to conduct global integrated operations at a speed and with a degree of precision that was unimaginable just a few decades earlier.[1]

Military power in the 21st Century will not be denominated according to the traditional units of account, tanks, planes and ships, but in terms of the breadth, sophistication, speed and security of the networks that empower a nation's or group's armed forces.

In order to more effectively, efficiently and securely exploit the advantages inherent in a networked force, the Department of Defense (DoD) is beginning to change the way it organizes and manages its networks. The Pentagon is building the Joint Information Environment (JIE), a single joint enterprise IT platform that can be leveraged for all DoD missions. It is designed to provide greater standardization, economies of scale, end-to-end visibility and a new, single security architecture.[2] The JIE envisions a single security architecture that will provide the organizational backbone, operational coherence, end-to-end situational awareness (SA) and rapid response needed to provide cyber security for the massive and growing IT environment.[3] The Defense Information Systems Agency's (DISA) *Cyber Strategy* calls for establishing an adequate level of end-to-end security for the defense enterprise overall, providing robust defenses for critical networks, protecting important data, ensuring the integrity of command and control, maintaining continuity of operations in a degraded environment and recovering rapidly.[4] Moreover, the defense department's vision for cyber security extends beyond networks and devices to embedded computing. According to the Pentagon's Deputy Chief Information Officer for Cyber Security, Richard Hale, "If there is a computer in something, it can be cyber-attacked, and we need to be able to harden it and defend it."[5]

Security cannot compromise the ability of networks to support military missions or of platforms and systems to perform as needed. DISA's strategic plan sees the future as "Authorized, authenticated user access and freedom of maneuver to cloud, collaboration, and command and control capabilities without impact from rogue entities, hacktivists, nation states, or insider threats."[6]

These are all good words. Now there must be action. DoD needs to implement its vision for the JIE. Similarly, DISA must invest in the structures, processes and technologies and human capital to support true end-to-end network surveillance and security. The sheer magnitude of the task dictates

[1] Admiral James A. Winnefeld Jr., "Remarks at the West Point Cyber Conference," West Point, May 14, 2015.
[2] U.S. Defense Information Systems Agency, *Enabling the Joint Information Environment*, May 5, 2014.
[3] Danielle Metz, Joint Information Environment Single Security Architecture, AFCEA, May 12, 2014.
[4] U.S. Defense Information Systems Agency, *Strategic Plan 2015-2020*, June 6, 2015.
[5] Sydney J. Freedberg, "Cybersecurity Now Key Requirement For All Weapons: DoD Cyber Chief ," *Breaking Defense*, January 27, 2015.
[6] DISA, *Strategic Plan 2015-2020*, *op.cit*.

a requirement for a coherent management framework and supporting systems, creating a "single pane of glass," for the purposes of surveillance, threat detection and response at network speed.

DoD is only beginning to develop the strategic wisdom, operational experience and military capabilities with which to prevail in the new cyber domain. The interplay of cyber offense and defense, intelligence and counter intelligence, deterrence, retaliation, and war waging in a networked world will require intensive thought, experimentation and analysis. What is known is that conflicts of the future, virtual and kinetic, will be different than those that have come before.[7]

Challenges to Effective and Secure Networks

General Keith Alexander (USA, Ret.), former Director of the National Security Agency and Commander, U.S. Cyber Command, has repeatedly warned of the threats to DoD's networks:

> *I look at the DoD Architectures today, and defending them is really hard. We have 15,000 enclaves, each individually managed. The consequence of that is that each one of those is patched and run like a separate fiefdom. The people who are responsible for defending them cannot see down beyond the firewalls. Host-based security systems are helping, but practically speaking, Situational Awareness (SA) is non-existent.*[8]

For an organization so dependent on its networks and which is guided by the Principles of War dictating, *inter alia*, the need for unity of command, economy of force and the centrality of the objective, the situation described above is untenable.[9] DoD networks are under continuous attack, 250,000 a day by some estimates, ranging from curious teens to the advanced persistent threat and malicious insiders.[10] The Director of National Intelligence's latest Worldwide Threat Assessment warned that the cyber threat was increasing in frequency, scale, sophistication and severity of impact, and that the ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding.[11] The DoD is not only threatened by attacks on its own networks but by those against government agencies with whom the Pentagon works, the private sector companies from whom it depends for a vast array of goods and services and portions of the nation's critical infrastructure on whom it is dependent.[12] Moreover, attackers have an inherent advantage: the defender must spend far more in order to have a reasonable chance of success. Based just on recent successful attacks on U.S. public and private networks attributable to foreign countries, it is easy to conclude that this country is in an ongoing, low-intensity war, albeit a virtual one, with a number of nation-state adversaries. [13]

---

[7] Kenneth Geers, *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence, June 2011, Chapter V.
[8] General Keith Alexander (USA), USCYBERCOM Commander and Director of NSA, "Interview to Federal News Radio," August 24, 2012.
[9] On the application of the principles of war to defense cyber operations see General Ronnie Hawkins, *Defensive Cyber Operations*, AFCEA, June 16, 2015. Also, Geers, *op. cit.*, chapter 6.
[10] U.S. Secretary of Defense Ashton Carter, Drell Lecture: "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," Stanford University, April 23, 2015.
[11] James R. Clapper, "Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee, February 26, 2015.
[12] Geers, *op. cit.*
[13] Georgia Institute of Technology, *Emerging Cyber Threats Report 2015*.

The evolving threat is only one of several challenges to DoD's efforts to create secure and effective networks. DoD's cyber enterprise is continually growing and changing. Today there are more than seven million devices on DoD's networks; tomorrow there will be many more. The use of mobile devices is becoming commonplace, even on the battlefield. Like the private sector, DoD is moving to the Cloud. The Internet of Things (IOT) is coming to DoD too. New devices, network technologies and applications inevitably introduce new security risks. A recent study by Hewlett Packard concluded that "attacks on Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on IOT devices."[14]

The department's efforts to expand its use of IT, organize its networks and enhance their security are challenged also by a lack of adequate resources. Defense budgets are declining and the demands for more resources from all sides are growing louder. Cyber security is not cheap. It is necessary to maintain and upgrade relevant legacy capabilities while simultaneously introducing new technologies and techniques. DoD needs a smart cyber acquisition strategy that avoids unnecessary expenditures while making sound investments in next generation capabilities. Such a strategy must recognize that there is much more involved in deploying a capable defense of the DoD joint enterprise than merely acquiring and installing software. This acquisition strategy needs to focus greater attention on training and service support to ensure that systems are installed and properly tuned to meet mission requirements. Just as cyber defenses must respond at network speed to be effective, so too must the associated acquisition system.

DoD's leadership recognizes that it faces a "cyber perfect storm" of evolving threats, expanding networks, rapidly changing technologies and declining resources.[15] DoD's advantage in network warfare will be short-lived and its investments in new capabilities for naught if the threats discussed above cannot be countered. Victory in future conflicts may go to the side best able to defend their networks from penetration, exploitation and attack.

Key Elements of a 21st Century Approach to Securing DoD's Networks

DISA has recognized the need to move to the next generation endpoint security. As it stated in a recent Request for Information to industry on a next generation endpoint security system:

> *The endpoint has evolved to encompass a complex hybrid environment of desktops, laptops, mobile devices, virtual endpoints, servers, and infrastructure, involving both public and private clouds. New technologies – including those for virtualization, workforce mobility, and Cloud services – are changing the way we conceptualize the desktop. DISA is requesting responses for innovative solutions to provide security services in heavily virtualized environments that provide economies over replicating security services in each virtual endpoint. Traditional approaches have used signature based defenses; however these methods have become un-scalable.*[16]

[14] Hewlett Packard, *Internet of Things Research Study*, September 2014.
[15] U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015.
[16] U.S. Defense Information Systems Agency, *Next Generation End Point Security System*, Solicitation Number: MAC0099, January 5, 2015.

This is a compelling but also a grand vision. The move from current approaches with their emphasis on signature-based defenses to robust end-point security will take time, new structures, innovative tactics, techniques, and procedures (TTPs) and resources to turn words into deeds. This is not a challenge that can be met overnight by the introduction of any "silver bullet" or by adding more cyber security specialists. Given the magnitude, complexity and cost associated with providing next generation endpoint security, DISA must take a strategic approach to this problem. Certainly, such a strategy must improve the security of DoD's networks. But it also must make the best use of scarce resources, consolidate activities, improve oversight and SA, provide the overarching structures to support measured modernization of its cyber security tools and TTPs, and reduce manpower demands.

Based just on recent successful attacks on U.S. public and private networks attributable to foreign countries, it is easy to conclude that this country is in an ongoing, low-intensity war, albeit a virtual one, with a number of nation-state adversaries.[13]

So, how should DoD proceed to create a 21st Century network security system? There must be leadership and accountability. Order needs to be imposed on a fragmented system. It is imperative that DoD consolidate networks, reduce fragmented control, eliminate redundancies, enable end-to-end SA and support responses to threats at speed. The decision to create the JIE with its single security architecture reflects a recognition of this reality.[17]

A single security architecture is only one of the keys to developing and operating a 21st Century network. Another is the capability to exercise centralized control, the organizational expression of the principle of unity of command. The ability to exercise necessary controls over the security of the entire JIE is particularly important when the proposed security architecture is open and there are requirements to integrate multiple vendors' products seamlessly and without introducing additional vulnerabilities. The JIE is an opportunity to architect the enterprise with security as an integral design element, in effect baking in security from the start as part of system design.

Almost by definition, a 21st Century security architecture must be open because it will be constantly evolving as outmoded software is removed, other features are modernized and entirely new technologies integrated. It is absolutely vital that it be built around a core management system, a platform, which provides policy-based system management, end-to-end visibility, real-time SA and rapid data sharing while simultaneously allowing users to reconfigure networks and make changes to security features without impacting the underlying framework.

Network consolidation, unified management and structured deployments of new capabilities are necessary, but are insufficient to meet the needs of 21st Century network security. A layered defense is required, one that builds on perimeter security and responsive vulnerability mitigation, but emphasizes an active defense that maintains the initiative by employing end-to-end surveillance, information sharing and continual observation and response. "Proactive policy-setting work – like patching Web-facing applications and utilities, reducing the number of applications to manage, removing administrator rights, and potentially exploiting application control – will, by itself, defeat 85% to 90% of malware."[18]

[17] *Under Cyber Attack: EY's Global Information Security Survey 2013*, EY, page 11.
[18] *Magic Quadrant Endpoint Protection Platforms*, Gartner Group, December 27, 2014.

However, emerging and future threats will require new and improved security technologies and techniques. The engagement between attacker and defender takes place over time. According to one reputable source that assessed a large number of attacks on private and commercial networks, 84 percent of attacks took only seconds, minutes, or hours to compromise their targets, while 78 percent of breaches took weeks, months, or years to discover.[19] So-called advanced persistent threats can conduct campaigns against high priority targets that persist for months, enduring even after initial countermeasures are introduced.[20] It is necessary to develop a strategy that addresses the threat's life cycle.

Getting to a Secure Network: Build on Success

It is clear that the JIE and the single security architecture will be built in stages.[21] The process will be evolutionary, taking what exists to create a consolidated and shared network infrastructure that will allow end-to-end connectivity as well as visibility while maintaining functionality and security. As new services and capabilities such as mobile devices and Cloud computing are added, existing security systems certainly will require modification to support a seamless security architecture.

The Defense Information Systems Agency has invested more than a decade and significant resources providing DoD's network with its first coordinated, department-wide security system, the core of which is the Host-Based Security System. HBSS is a commercial off-the-shelf (COTS) based integrated application suite that has undergone rigorous security, functionality and compatibility testing that proved its effectiveness on more than seven million endpoints. In two contracts, one each with BAE Systems and Northrop Grumman, DISA invested some $400 million to deploy HBSS and train personnel. The military services have added $100 million or more to this amount. When properly managed, with trained operators, kept up to date, with settings at appropriate levels, and fully implemented, HBSS is reported to be extremely effective against today's spectrum of threats.

It is clear that DISA intends to move beyond host-based security to next generation end-point security. But it must do so in a way that leverages the best of its current capabilities while simultaneously creating a new, more effective and responsive security system. New devices, network technologies and security capabilities must be integrated into an overall next generation security system. The question is managing the transition while maintaining the current level of security and avoiding unnecessary costs and delays. When undertaking a large complex program there is always a temptation to start anew, tossing aside existing capabilities and their sunk costs in favor of that which appears new and different. This approach presents three difficulties. First, it almost certainly comes with additional costs as current and functional systems are removed and new ones installed. There is the additional cost of retraining the workforce. Second, this adds to the risk of schedule slippage due to the need to ensure interoperability and demonstrate functionality. Third, additional uncertainty is injected into the system as the number of new and untested security suites are expanded. There are cyber security challenges enough with consolidation, new devices, Cloud computing and new architecture without adding risk by redoing the installed base. The tendency to

[19] *Verizon 2013 Data Breach Investigation Report, 2013*, pp. 50-52.
[20] *Lifecycle of an Advanced Persistent Threat*, Dell SecureWorks, 2012.
[21] U.S. Department of Defense, *The Department of Defense Strategy for Implementing the Joint Information Environment*, September 18, 2013.

gravitate to the new and untested assumes that these must be better options largely because they are novel.

Any security strategy needs to build on current successful investments and experience in order to avoid introducing risks and incurring additional costs even as new technologies and techniques are added. The baseline of currently deployed capabilities is still relevant. Moreover, they have been thoroughly tested and vetted in the real world. If properly maintained and updated, they permit security to focus greater attention and resources on more challenging tasks such as mitigating the advanced persistent threat or new vectors of attack. In addition, currently deployed security controls can be leveraged and repurposed to provide additional defenses.

Faced with an enormous mission but limited by available resources, it is important that DISA take advantage where possible of its existing investments in security capabilities rather than attempting to wipe the slate clean. It is clear that existing security solutions continue to provide value, certainly if properly maintained. They represent a large installed base supported by an experienced workforce (both government and contractor). The core values of DISA's current approach to network security – centralization, scalability, configuration control and end-to-end visibility – have to be upheld, even as security is extended to the Cloud, to the IOT, and to the tactical edge where bandwidth is scarce and network vulnerabilities are not the top issue on users' minds.

Getting to a Secure Network: A 21st Century Security Architecture

Meeting the multiple challenges involved in protecting a massive, complex and changing information enterprise effectively and efficiently necessitates the creation of an overarching DoD security architecture. The JIE's proposed single security architecture is intended to address many of the limitations of the current disaggregated approaches, providing standardized security suites at optimal locations, eliminating redundant/obsolete protections, controlling user data flows and enabling global SA, protecting enclaves after the separation of server and user assets, and providing the tool sets necessary to monitor and control all security mechanisms.[22] According to Mark Orndorff, then-chief information assurance executive and program executive officer for mission assurance and network operations at DISA:

> *The No. 1 most important advantage (of the single security architecture) is the ability to actively defend the DOD networks in a time frame that we need to execute cyber defensive operations. What I mean by that is the single security architecture will allow us to understand what's going on across the entire DOD network with global cyber situational awareness to a level that we can't do today.*[23]

But in order to achieve the JIE's vision and meet the myriad challenges facing the effort to provide enterprise security, the single architecture must be open, reflecting the value of accessing a variety of vendors, but also based on a single platform and unified framework to insure connectivity across security technologies. In addition, there must be tight high-level configuration controls, appropriate standards and protocols and verification procedures for new applications. In its 2010 report on

[22] Danielle Metz, *The Joint Information Environment Single Security Architecture, op.cit.*
[23] Greg Slabodkin, "Defending DOD networks with a single security architecture," *Defense Systems*, July 19, 2013.

network resilience, the Defense Science Board recommended that DoD "Establish an enterprise security architecture, including appropriate 'Building Codes and Standards,' which ensure the availability of enabling enterprise missions."[24] Codes and standards apply not only to new applications but to security processes, organization and training.

A unified DoD IT enterprise and supporting security architecture is critical to the introduction of new security strategies and TTPs. It is already clear that the locus of security for large, complex networks is shifting from perimeter defense to a layered defense operating simultaneously across the entire structure. In addition, the security architecture must support reductions in the overall time from penetration to detection to resolution. Much value can be achieved if the dwell time of hostile actors inside the network is significantly reduced. This requires end-to-end visibility, real-time threat intelligence, robust information sharing, extreme rapid threat detection and responses to threats at network speed. This architecture must drive towards simplicity and automation. The concept of middleware, or a connected "nervous system" is required to address the challenges of today and tomorrow at network speed.

Comprehensive training is essential for any complex system. When the Army purchases a fleet of Stryker combat vehicles, for example, all those who will operate the vehicle go through an extensive course of training and preparation. For any security system to be effective, serve as part of an integrated military force or even an effective weapons system, its personnel must be trained on every aspect of its features and capabilities. Moreover, like any complex kinetic weapon system, security systems must be installed, tuned, and serviced in a rigorous manner. This is particularly important in tactical environments, where the military is challenged by having to stand up facilities in new zones – sometimes combat zones – with lower bandwidths and other sub-optimal conditions. Absent the training, tuning, and services, the system is not operating in its optimum capacity, and the DoD is not getting the full value of its investment.

This architecture also must respond to the introduction of new users and new devices/endpoints, as well as the rapid addition of new security capabilities with no loss of functionality. The increased use of mobile devices further challenges network security which often does a good job defending endpoints in garrison, but faces a more difficult and fast changing set of problems when military forces are deployed.

Getting to a Secure Network: Designing a Single Management Construct

The JIE's single security architecture serves as a solid framework, even a skeleton, around which DoD will be able to build the entire living IT enterprise. This architecture provides the backbone on which a comprehensive, flexible and responsive security system can be built. The networks themselves are like the nervous system, providing the flow of information throughout the enterprise.

What still must be added is a clear, integrated management capability that will help DISA and security managers exercise leadership and direction. Stovepiped security organization, fragmented responsibilities and inconsistent procedures, protocols and rules can render any security system relatively brittle. Without the proper management platform with which to coordinate the

[24] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013, p. 56.

introduction and operation of a wide range of security tools and techniques, the overall security architecture is in danger of fragmenting or, at a minimum, introducing new vulnerabilities. There must be an overall system management construct, the guiding brain of the security enterprise to assist decision makers by providing end-to-end, real-time SA and the capability to oversee implementation of the new security system and the introduction of new technologies and TTPs.

Almost by definition, a 21st Century security architecture must be open because it will be constantly evolving as outmoded software is removed, other features are modernized and entirely new technologies integrated.

Given the scale and complexity of DoD's networks, the breadth of security protections and techniques employed by users, the demands to modernize the provision of security and the need to ensure integration of security capabilities as consolidation proceeds, it is imperative that there be an overall system management capability. This is a lesson learned at considerable cost by the Navy in its NextGen communications program, the Soltra joint venture between the Department of Homeland Security and the financial industry, and the British Ministry of Defense's Atlas consortium that manages its Defense Information Infrastructure. The JIE strategy seeks to incorporate this lesson in the development of a single security architecture.

> *One of the core elements of JIE is that DoD network operators and defenders must work as one team. The JIE will enable network and system operators and defenders at every level to have visibility into the status of the networks, as well as enable commonality in how cyber threats are countered by DoD. The Department will know who is operating on its networks and what they are doing, and it will be able to attribute their actions with a high degree of confidence.*[25]

Achieving the goal of unified operations requires a common management system and supporting set of tools accessible by all network operators. A systems management approach would support the maintenance of configuration control while advancing security capabilities across networks. This function is vital in order to address advanced structured attacks. A single management overlay will ensure the viability of legacy products and the easy integration of new products or services with existing capabilities, as well as supporting the inevitable evolution of the enterprise as missions, threats and technologies evolve. In addition, the single management platform must be tasked to think and plan strategically for the inclusion of new devices (e.g., mobile) and introduction of new security technologies.

An overarching management construct also will assist DoD in realizing its goals of increased overall enterprise effectiveness and efficiency in the provision of services, particularly security. In close collaboration with the government, the single management system can find its way across the challenging landscape of DoD enterprise security. In particular, looking ahead, applying a common set of management tools and design principles will support the efficient allocation of resources while avoiding redundancies and even conflicts. Even more important, the common security construct can assist DISA and system administrators in their efforts to ensure that all the proper security procedures and protocols are maintained in the face of any resistance from the users. This

[25] *The Department of Defense Strategy for Implementing the Joint Information Environment, op. cit.*

will enable those with the responsibility for providing network security to sustain the priority of security over user behaviors that may place networks at risk.

Now is the time for DoD to think long-term and optimize the enterprise, networks and security architecture for growth, reduced risk of surprise and maximum operational flexibility. A single management platform for that architecture with experience providing security for large, complex government networks and a deep understanding of cyber technologies could best help DoD in this endeavor.

Getting to a Secure Network: Advance the Defense as the Threat Evolves

In 2010, the Defense Science Board published a study on how DoD could create and maintain resilient military systems. The study concluded, in part, that:

> *Cyber is a complicated domain. There is no silver bullet that will eliminate the threats inherent to leveraging cyber as a force multiplier, and it is impossible to completely defend against the most sophisticated cyber threats. However, solving this problem is analogous to solving complex national security and military problems of the past … The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed.*[26]

Cyber security is the quintessential competitive strategy in which each offensive action produces a corresponding defensive measure which, in turn, propels the offense to renew its search of another avenue of advance. In essence, this means that there is a life cycle to the threat, one in which it interacts with the network and its security systems over some period of time. The need for newer, more capable cyber solutions will be continually driven first and foremost by changes in threats, but also by the development of new network designs and management strategies, the addition of new network technologies and even by changes in cyber security capabilities such as next-generation non-host-based security technologies. For example, many first-generation solutions were designed for slow and historical situational analysis, rather than the "in the moment" SA that is required today. Similarly, perimeter security strategies made sense when networks were relatively simple, with only slow growth in the number of users and the introduction of new device technologies. Now they make much less sense as the world is encrypting a significant and growing amount of network traffic, preventing inspection in real-time.

Ironically, most attacks against government and civilian networks conform to a relatively small number of patterns. Two threats that continue to stress security systems are the so-called advanced, persistent adversaries and the malicious insider. These challenges can't be met simply by building higher walls to prevent intrusion. Security must be more pro-active rather than reactive and cover the entire network life cycle. New technologies and TTPs are needed to detect anomalous behavior, minimize the duration of successful intrusions and mitigate the effects of successful attacks.

[26] Memorandum of Transmittal to the Defense Science Board, *Final Report of the Defense Science Board (DSB) Task Force on Resilient Military Systems*, October 10, 2012.

The consolidation of the DoD information networks into the JIE, the reduction in data centers and the creation of Regional Security Stacks practically dictates a parallel consolidation and centralization of security management. Properly managed, the centralization of security will go hand-in-hand with the development of end-to-end visibility, real time SA, rapid anomaly detection and swift neutralization of penetrations.

New cyber technologies will both challenge and enhance the ability to implement layered security strategies. The proliferation of mobile devices has outpaced the development of their security systems. New approaches are needed. On the positive side, there is enormous potential benefit to be had in host-based security and even in hardware enabled protective features.

It is clear that DoD needs cyber solutions that will grow and adapt as threats change. Contracts with security providers must be written in a new way, one that reflects the need for flexibility, provides for rapid response to changing threats, and allows for timely exploitation of SA and threat information from sources outside of the JIE.

Getting to a Secure Network: Automated Sense and Response

The sheer size of DoD's array of networks, their continually changing character, the increasing speed at which information is moving on its networks and the growing sophistication of threats has already made it impossible to provide the required level of SA and timely sense and response to intrusions solely with human security personnel. The ability to counter sophisticated threats employing purpose-built tools and targeted malware will require the extensive use of automated detection and response systems and adaptive threat prevention routines operating at network speeds.

The effort to create the JIE and the single security architecture opens the way for the implementation of protocols and systems that will allow cyber information to be collected, analyzed and exploited by automated systems, enabling better security command and control and reducing the amount of human touch required to provide security. Automated patch management alone can substantially reduce the manpower requirements associated with security system maintenance. According to the Defense Science Board study on *Resilient Military Systems and the Advanced Cyber Threat*,

> *Commercial technologies that enable the automation of some network maintenance activities and provide real-time mitigation of detected malware are available today. The Task Force believes that use of these technologies would actually drive network operation costs down and free up resources to hunt on the network for intruders.*[27]

The future DoD cyber security environment will need methods that allow a wide variety of security tools to communicate with one another, share security information from all sources that is both relevant and timely, and synchronize real-time intelligence and response. Security providers are continually struggling to keep abreast of the sheer volume of threat data as well as the changing character of network attacks. The only way to get ahead of these problems is by greater investment in automation to address such tasks as advanced malware analytics, intelligent algorithms, system

[27] Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013, p.9.

modeling, anomalous behaviors by insiders, and the continual development of intelligence information on potential penetrations and attackers' TTPs. Such a level of automation could eliminate traditional product silos, allowing for a level and speed of information sharing heretofore impossible to achieve.

Automation will also be critical to dealing effectively with intrusions. Minimizing the impact of an attack is a time-consuming task. Once an attacker has successfully penetrated a target, there is a finite amount of time before significant damage is done or critical information extracted. Automated threat detection, analytics and anomaly characterization can speed up the response process and free critical personnel for more important tasks.

To date, organizations, including governments, have approached cyber security as an add-on to traditional IT functions. It is time to re-imagine cyber security as an inherent element of all network operations.

The automation of time-consuming and manpower intensive processes not only can accelerate security efforts but also produce significant cost reductions. Automation not only reduces personnel levels but also can simplify training requirements.

There is an inextricable relationship between network expansion and the need for greater automation driving, in turn, new demands on the networks themselves. Management of future security architectures must take these into account when building new security capabilities.

Getting to a Secure Network: Exploit Commercial Security

As Secretary of Defense Ashton Carter acknowledged in his speech at Stanford University, the locus of research and development investment in IT, generally, and cyber security capabilities, in particular, had shifted from the public to the private sector. The private sector has established an extremely rapid pace of innovation. This compares with the government's increasingly lethargic pace of technological innovation and the growing burden of the acquisition process.

Expanding the effectiveness and coverage of cyber security systems in a timely manner must exploit commercially available products and experience. Private companies have the relevant experience creating and maintaining security systems for well-established environments with infrastructure that cannot be rebuilt from the ground up. They also have experience in providing security solutions for extremely large, complex environments and from chips to the Cloud. This point was driven home recently by Admiral James Winnefeld:

> *… we desperately need the help of industry to speed our passage into a new paradigm of cybersecurity dominated by technologies other than signature-based detection. This is a Big Data problem that connects data, analytics, placement and visualization within a complex ecosystem of ISPs [internet service providers], cyber security firms, software providers, hardware manufacturers, and data storage companies.*[28]

[28] Winnefeld, *op.cit.*

Commercial cyber companies are experienced in developing affordable as well as effective solutions. The private sector cyber security providers have developed solutions to most of the challenges facing government Chief Information Officers and network security managers. Private companies have developed systems and TTPs with which to address the evolution of complex information environments, the creation of single management system, the consolidation of functions, the integration of individual security measures and technologies, application control and data sharing.[29]

The private sector has demonstrated an ability to rapidly develop, field and integrate new solutions. Given the pace at which the threat is evolving, this is critically important to managing the problem. In addition, DoD and other federal agencies need to leverage ongoing investments by the private sector in security technologies. But in so doing, it is important to internalize the lessons from repeated failed efforts to adapt commercial enterprise resource planning systems to the unique processes and rules of the government. To take advantage of the cyber security products and services the private sector has to offer, DoD will have to change some of the way it is organized, procures, and behaves with respect to cyber security.

DoD needs to study the methods employed by the private sector to reduce manpower usage and other costs associated with cyber security. The challenges facing commercial companies in 2015 are not materially different from those facing the DoD and government. It must leverage commercial IT products and services if it is to reduce the costs for cyber security and improve overall security effectiveness.

Evolving to a 21st Century Network Security System

We are witnessing an inflection point in information architectures and cyber security. Networks are becoming larger, more involved and complex. The U.S. military is more dependent than ever on its networks. But threats advancing at a dangerous pace could overwhelm current cyber defenses. In addition there needs to be a reformulation of strategies for providing security. Perimeter security and antivirus protection are still necessary, but insufficient by themselves. A change of mindset is required.[30]

This new mindset must start with an appreciation both of where the department is today with respect to cyber security and the distance it has yet to travel to reach its goals. DoD has invested significant resources, both financial and human in its current endpoint security system. This system has demonstrated its effectiveness. It makes sense to build out from the core of the existing system, utilizing its framework, management capabilities and resources as a foundation for the evolution to a next generation. Existing security capabilities need to be upgraded where possible, scaling signature based technologies to cheaply remove known threats. Newer techniques are necessary in order to better address merging threats and to provide enhanced initial layers of defense.

Equally important, network security managers must be willing to make sufficient investments in training and consulting to ensure that systems are installed and properly tuned to meet mission

[29] *Magic Quadrant for Endpoint Protection Platform, op.cit.*
[30] Sarah Kuranda, "RSA President: We're At A Security Inflection Point, But Not On A Path To Win," CRN, April 21, 2015.

requirements. Too often, DoD organizations invest in security software but not in the training related to maintaining critical systems and responding to anomalies.

Rather than focusing narrowly on adding security products to the existing system, potentially layering new solutions on top of old ones, a 21st Century approach to network security needs to be based on an overarching architecture. A single architecture is important to configuration control, training standards, and the implementation of planned rollouts of upgrades and new technologies. It is critical also, along with the empowerment of a single manager, to achieving the operational requirements for next generation security such as end-to-end, full stack SA, the creation of a common operational picture, integration of threat and intelligence information and rapid response to anomaly detection or identified intrusions. The architecture can be built around a core of common data centers, shared services, regional security stacks, and the migration/integration of an approved and tested set of security technologies. This will concentrate security where network use is greatest and provide a basis for identifying any security gaps that require the introduction of new security technologies.

The continuing expansion and evolution of DoD networks, the creation of the JIE and overall system consolidation demands a new level of leadership, oversight and responsibility. This can only be found in the creation of a single management platform for security of the DoD enterprise. A single management platform is important to the creation of an overarching architecture and the implementation of system-wide security protocols and standards even in the face of contrary user behaviors. Systems administrators are empowered by the SA and configuration controls that such a platform can provide, particularly in the early stages of transitioning to next generation security. Centralized management supports system-wide visibility, an ability to monitor asset deployment and employment, end-to-end monitoring of the security of every endpoint and the ability to understand security events on a system level. The single management platform is where policy issues such as boundary management, network access, identity management, training standards and threat warning and response can be determined. Given modern security tools and techniques and the level of automation available through COTS, this must be a thin management layer that does not inhibit flexibility on the part of individual systems administrators or managers of specific networks and regional security stacks.

A single security architecture and common management platform are the necessary antecedents for any strategy that seeks to continually advance security as the threat evolves. With these structures in place and a foundational set of security technologies already utilized, it is possible to systematically deploy new capabilities in a structured and cost-effective way. Specifically, security needs to be seamlessly extended to include mobile devices, Cloud services and virtualization technologies. In addition, efforts need to begin to develop and validate hardware and even chip-embedded security technologies.

It is obvious that securing critical networks, data and functions against the massive and evolving cyber threat will require an unparalleled degree of automated threat detection and mitigation. There needs to be a clearly articulated plan and set of processes to move forward on automating network security activities. Automation will support the creation of more stringent controls, increase the speed of diagnostic and mitigation activities and reduce network and system administration costs. The initial foci should be on those activities that are manpower intensive or require speeds beyond what is possible for security specialists.

DISA has proven the value of adapting COTS products to the needs of DoD network security. Clearly, reliance on commercial products is the way forward to a cost-effective security system. Leveraging the power of the commercial sector more effectively means early involvement by private companies in the development of a single open security architecture. It is imperative that DoD develop a new, rapid and flexible acquisition system for cyber security capabilities. It would be useful also to examine ways of swiftly identifying, assessing and acquiring new technologies in response to urgent security requirements.

To date, organizations, including governments, have approached cyber security as an add-on to traditional IT functions. It is time to re-imagine cyber security as an inherent element of all network operations. Cyber security must evolve to a comprehensive, dynamic and flexible set of processes and practices that integrate hardware, software, organizations, behaviors and people for the purpose of deterring, denying and defeating threats to critical networks. Cyber security must be built into every network, system and even processor. Good security practices must be inculcated into every network user, not just the system administrators. Like any large, complex human system, network security will evolve over the lifetime of the information enterprise. Hence, DoD must invest in the comprehensive training and services from an elite squad of cyber security professionals in order to realize the full value of high-end security capabilities across the entire DoD enterprise. In addition, DoD organizations and cyber security managers will have to address the inevitable life cycle issues associated with the introduction, deployment, modification, extension, upgrade and, eventually, obsolescence of a security system.

Glossary of Terms

DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense
COTS	Commercial Off-The-Shelf
HBSS	Host-Based Security System
IOT	Internet of Things
IT	Information Technology
JIE	Joint Information Environment
SA	Situational Awareness
TTP	Tactics, Techniques, and Procedures

Lexington Institute

1600 Wilson Boulevard, Suite 203 | Arlington, Virginia 22209
Tel: 703-522-5828 | Fax: 703-522-5837
Email: mail@lexingtoninstitute.org