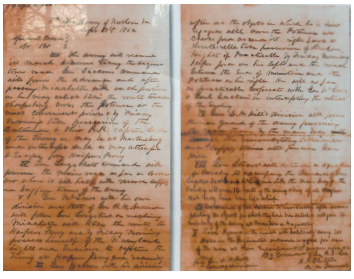
WHITE PAPER

# Multi-Layer Security: An Approach to Protecting Intelligence in Cyberspace

***July 2012***

*Conventional security standards and practices cannot keep up with the frequency and sophistication of attacks.*

## Introduction



In September of 1862, a battle that Civil War historians consider to be at least as pivotal as Gettysburg was fought at Antietam. The chance discovery by Union forces of Robert E. Lee's secret orders, dropped in a Maryland field, revealed that Lee had divided his force. That gave the Union army of 80,000, under Gen. George McClellan, a chance to intercept Lee, who had only 35,000 men to bring into the battle.[1]

Fast forward to June 2012, when it is revealed that the United States and Israel jointly developed a sophisticated computer virus nicknamed Flame that collected intelligence in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon.[2]

The theater of operations has expanded and evolved dramatically in the last 150 years. And the importance of secrecy, intelligence and rapid organization and collaboration among many resources is as important as ever. Successful outcomes require information sharing at a scale, speed and reach never before seen.

Support for all such missions requires a secure, reliable global network capable of transporting extremely large amounts of data, challenges that the DoD Information Enterprise is designed to take on. Helping ensure the safety of warfighters and effective collaboration among multiple agencies calls for an evolving infrastructure that's capable of countering increasingly sophisticated cyberattacks, and can also leverage economic and productivity enhancing technologies such as the cloud and those that enable unified communications.

In this paper, we discuss the evolving role that telecommunications plays in fulfilling the DoD's missions and offer our perspective on how a multi-layer security strategy can help manage threats. We will examine some of the economic and political drivers and highlight key technologies that will help meet new demands for efficient information exchange.

Just as Generals Lee and McClellan understood in 1862, security of that information exchange can determine the outcome of a battle and perhaps a war. Throughout this paper, we will place a special focus on cybersecurity, because the issue at hand is not "if" cyberattacks will occur; it is how to prepare for "when."

## Economic and Political Drivers

The U.S. Federal Government is projected to spend $79.5 billion on IT in fiscal 2012; of that, $38.2 billion is earmarked for the Department of Defense. The proposed federal IT budget for FY 2013 is $78.9 billion, a 0.7 percent reduction.[3] Responding

*Answering to the voice of the people, federal legislation has been enacted to stimulate the economy and rein in accelerating costs.*

to pressure to help reduce the overall federal deficit, the DoD continues to use resources more efficiently while simultaneously improving its capabilities and mission outcomes.

One avenue for cost reduction is modernization, which primarily means using technologies that help streamline processes and eliminate redundancy. Modernization is not specific to warfighters. The multiple agencies that comprise the DoD are included in the IT spend and, just like private enterprise, they also face IT issues such as Big Data, the impacts (positive and negative) of mobility, cybersecurity, and changing leadership.

The Great Recession of 2008 has forever altered the way Americans view government spending. Answering to the voice of the people, federal legislation has been enacted to stimulate the economy and rein in accelerating costs. Agencies are being consolidated and, in some cases, dissolved. IT projects are being reprioritized, with those that curb costs or even generate revenue stepping in front of those deemed "nice to have." There's a greater emphasis on privatizing programs and outsourcing IT activities such that best-in-class organizations supplant resources otherwise provided by government agencies. This also creates a competitive environment that naturally drives down costs, as each vendor is regularly evaluated and compared to its competition.

To sum up, all government agencies are intensely focused on controlling costs and are looking to established and emerging technologies to help them gain that control.

## The Global Cyber War

Protecting assets, safeguarding information and maintaining operations has taken on new meaning: It now encompasses IT equipment, massive amounts of sensitive data and uninterrupted private and public network communications. In fact, cybersecurity is the top concern of federal CIOs, according to results of a survey conducted by TechAmerica that was more widely distributed in Information Week.[4] Their concerns are based on some startling facts:

- Websites operated by organizations such as the CIA, the U.S. Senate, PBS and Citibank have been defaced in high-profile attacks by a hacking group called "LulzSec" (hacking for laughs).[5]
- 5.5 billion attacks were blocked in 2011 vs. 3 billion in 2010.[6]
- 315 new mobile vulnerabilities were detected in 2011 vs. 163 in 2010.[6]
- The number of attacks on federal agencies has increased from 5,503 in 2006 to 41,776 in 2010.[7]
- Infragard, an FBI-led partner organization, was compromised by hackers in Connecticut and Atlanta, revealing passwords of hundreds of industry and law enforcement users.[8]
- There are 30,000 new infected web pages every day — one every 2 to 3 seconds.[9]

These are only a small sample of the daily attacks. While technical innovation can provide better solutions for cybersecurity, such as more computing power for packet inspection within firewalls, it also can result in new areas where attacks can be made. Cloud computing, mobility and vulnerabilities created by

new (but less than bulletproof) software give foreign governments, organized crime, hactivists and professional hackers more opportunities to obtain classified intelligence or bring down networks.

## The Cloud

Cloud computing promises cost reductions, improved agility and innovation. Delivering software as a service (SaaS), enabling almost instantaneous data storage with minimal capital investment, and helping teams of people who are next door to one another or thousands of miles apart communicate economically are just a few reasons why agencies are looking to the cloud. Recognizing this potential, U.S. Chief Information Officer Vivek Kundra announced the Cloud First policy in 2011. According to the report outlining that initiative, $20 billion of the $80 billion spent on IT by the government potentially could be moved to the cloud.

*Cloud computing, mobility and vulnerabilities created by new (but less than bullet-proof) software give foreign governments, organized crime, hactivists and professional hackers more opportunities to obtain classified intelligence or bring down networks.*

Hackers target cloud computing companies, which can provide prime opportunities for gaining access to multiple agencies at once. Undaunted, in May 2012, federal CIO Steven VanRoekel launched the Shared Services Mandate. The strategy aims to help agencies reduce what they spend on redundant IT systems and services and allocate that money into new technologies and tech-enabled innovations. In the area of supply chain management, for example, the Office of Management and Budget (OMB) identified redundancies in 759 planned IT projects, valued at $3.3 billion. Leveraging collaboration technologies that can be implemented through the cloud, the OMB and other agencies will also work to reduce redundancies, help government staff become more productive and "free up people to put them on more important tasks."[10]

The general business case for cloud deployments is continuing to take shape. Organizations evaluating cloud versus on-premises strategies should keep in mind that a DIY approach can have merit, but the capital investment and costs of service associated with owning and operating the equipment can be unpredictable. In contrast, the economic model for an outsourced cloud strategy might show that the costs per year are higher, but the risk is lower and the expense is predictable.

*Hackers see cloud computing companies as prime targets to gain access to multiple agencies at once.*

Many agencies overlook that cloud computing is a service delivery model. Cloud computing largely uses existing virtualization and sharing technologies to deliver IT services in a way that are more economical and elastic. The use of cloud-based services shifts the IT burden away from maintaining physical servers and data centers, but this means that IT must more closely manage the telecommunications links used to access cloud-based systems and software. The cloud can create significant systems efficiencies and help with continuity, but agencies should still carefully consider the possible need for more telecommunications bandwidth.

Since both public and private cloud computing often rely on distributed computing, additional cybersecurity risks can be introduced in the form of Distributed Denial of Service (DDoS) attacks. These attacks are designed to block information exchange, much like radio jamming is used on the battlefield.

Radio jamming systems, once triangulated, are easily eliminated in minutes. However, DDoS attacks are usually initiated by BOTnets that are created from hundreds or thousands of malware-infected PCs. Tracking down and disabling a DDoS attack can take days.

*Drones and Big Data*

*Just how much data is streaming back to us?*

*"The Air Force has more drones and more sensors collecting more data than it has humans to interpret what the electronic tea leaves say."*

http://www.wired.com/dangerroom/2012/04/air-force-drone-data/

## Mobility & Big Data

Wireless networking has led to a sea change in the way people work in enterprise and the DoD. The DoD has developed a mobile device strategy aimed at embracing mobility. In a press release on June 15, 2012, Teri Takai, Department of Defense CIO, announced that new strategy, saying, "The Department of Defense is taking a leadership role in leveraging mobile device technology to improve information sharing, collaboration and efficiencies. As today's DoD personnel become increasingly mobile, a wide variety of devices offers unprecedented opportunities to advance the operational effectiveness of the DoD workforce. This strategy will allow mobile activities across the department to converge towards a common vision and approach."[11]

But mobility is not just about wireless connectivity. It also encompasses remote connectivity into private VPNs to support telecommuting and the changing nature of how work gets done. That connectivity is meaningless if it doesn't also connect the user to data and applications. Networks and data centers need to be highly available to be of any real advantage.

In addition, the issue known as Big Data is tied to mobility, security and network capability. Just like enterprises are seeking ways to absorb and analyze the influx of data resulting from the Internet, the equipment enabling command and control (as well as drones and other automated warfighting technologies) stream huge amounts of data — including weather, surveillance, target-acquisition and reconnaissance information — that need to be rapidly stored, analyzed and acted upon.

## Security Strategy Approach: Level 3's Vision

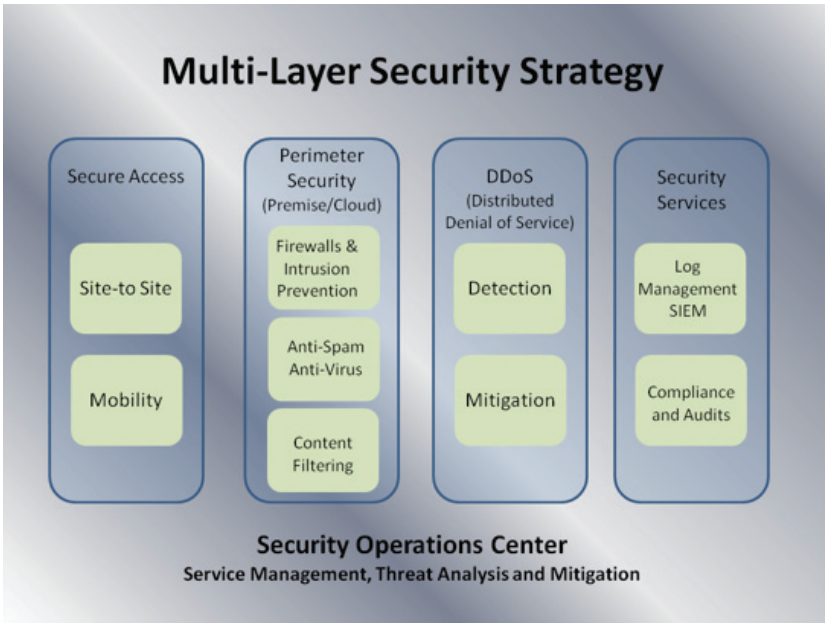
Considering the volume and ever-evolving nature of cyberattacks, virus protection software and firewalls can't adequately protect infrastructure and data. Threat management has become a near-real-time job that requires extensive resources to continually monitor, collect and analyze massive volumes of security event data. Furthermore, changing compliance requirements — including FISMA, HIPAA, Trusted Internet Connection (TIC), Cyberscope, and the Homeland Security Presidential Directive [12] — add to the burden of IT personnel.

Ideally, cyberattacks are detected and mitigated before they can take effect. A multi-layered cybersecurity strategy can help make this happen. A critical part of the scenario is extensive visibility into the network traffic, which can be established and monitored at a security operations center (SOC). The effectiveness of a SOC is directly influenced by the ability of its team of network management professionals to recognize nefarious behavior in the network. A SOC has access to tremendous amounts of network traffic statistics. These statistics are processed by an extensive set of rules that are used to identify traffic patterns, fraudulent data packets and other anomalies. These rules are developed over time and are constantly improved. The more broadly the SOC team can observe network behavior, the more effective the rules become.

In a multi-layer, unified threat management scenario, threat analysis, mitigation and service management begins with perimeter security. Providing secure site-to-site access and enabling secure remote access occurs in the firewall,

the first layer. Firewalls provide intrusion detection, but they also can provide inspection of traffic. The level of inspection can be dictated and varied, with policy scripts written to align inspection with the security requirements. This first layer includes anti-spam and anti-virus protection and content filtering as well.

*Firewalls provide intrusion detection, but they also can provide inspection of traffic.*




The second layer of protection is designed to address DDoS attacks. These BOTnet-facilitated attacks are becoming more powerful and faster. Compared to Q1 2011, there has been a:

- 25 percent increase in total number of DDoS attacks
- 25 percent increase in Layer 7 (application layer) DDoS attacks
- Six-fold increase in average DDoS attack speed[13]

With comprehensive network activity monitoring and virtually real-time global awareness of new attacks, DDoS attacks can be addressed.

The final layer of security includes the services that security professionals can provide. In addition to addressing compliance and auditing, these services deliver security incident and event management. Heuristic analysis of logs enables detection of previously unknown viruses; however, it's important to keep in mind that pattern analysis and anomaly detection is an evolving methodology. This service, like other cybersecurity services, calls for specialized expertise, which might compel an agency to engage a service provider.

*"Level 3 has pledged to work with other ISPs on specific detection, prevention, and tracing options that can be deployed industry-wide."*

## Conclusion

Evolving sources of threats and more skilled enemies. Shifting mandates and an unstable global economy. Evolving uses of technology, which create advantages and vulnerabilities. These are some of the variables that form the complex cybersecurity equation.

In addition to a range of adversities in the macro environment, the DoD must also consider the impact on specific combat missions and, finally, the individual warfighter. The individual and collective effort of warfighters can never be discounted, but history shows that intelligence can dictate the outcome of each mission. The tools of war have evolved to an amazing point of precision and destructive capability, probably far beyond the dreams of Sun Tzu. The value of intelligence, however, has not changed, and did not escape his understanding:

*Secret operations are essential in war; upon them the army relies to make its every move.*

The Art of War

As a global Internet Service Provider, Level 3 witnesses many attacks on a daily basis. Consequently we have the opportunity to analyze more data, and as a charter member of the ISP Security Consortium, Level 3 has pledged to work with other ISPs on specific detection, prevention, and tracing options that can be deployed industry-wide. As part of that commitment, Level 3 CEO Jim Crowe is serving as Chair of the National Telecommunications Security Advisory Committee, a group of chief executives of technology companies that advises the President of the United States concerning matters of national telecommunications security.

References:

1. Tony Horowitz, "On the War Path," National Geographic Traveler, June/July 2012, 74.
2. Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say," The Washington Post, June 19, 2012.
3. John Foley, "The Time Has Come for an IT Savings Dashboard," InformationWeek Government, June 2012, 3.
4. Therese Reger, "Security Top Concern of Federal CIOs," InformationWeek Government, May 8, 2012, http://www.informationweek.com/news/government/security/232901580.
5. Amy Lee, "LulzSec, Anonymous Hacker Groups Declare War Against Governments, 'Gluttons'," The Huffington Post, June 20, 2011, http://www.huffingtonpost.com/2011/06/20/lulzsec-anonymous-war-_n_880637.html.
6. Symantec Internet Security Threat Report – 2011, Symantec, http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers.
7. 2012 National Preparedness Report, U.S. Department of Homeland Security, March 30, 2012, 20.
8. Raphael G. Satter, "FBI Partner InfraGard Hacked, Passwords Stolen, LulzSec Claims Credit," The Huffington Post, June 5, 2011, http://www.huffingtonpost.com/2011/06/06/fbi-infragard-hack-lulzsec_n_871645.html.
9. "Sophos Security Threat Report 2011," Saphos, http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx, 37.
10. J. Nicholas Hoover, "The Shared Services Mandate," Information Week Government, June 2012, 9.
11. "DoD Releases Mobility Device Strategy," U.S. Department of Defense, June 15, 2012, http://www.defense.gov/releases/release.aspx?releaseid=15376.
12. Spencer Ackerman, "Air Force Chief: It'll be 'Years' Before We Catch Up on Drone Data," Wired, April 5, 2012, www.wired.com/dangerroom/2012/04/air-force-drone-data/.
13. Q1 2012 Prolexic Attack Report, Prolexic, http://www.prolexic.com/knowledge-center.html#tab4.