The US Army War College Quarterly: Parameters

Volume 41
Number 3 *Parameters Autumn 2011*

Article 3

8-1-2011

A Strategic Approach to Network Defense: Framing the Cloud

Timothy K. Buennemeyer

A Strategic Approach to Network Defense: Framing the Cloud

Timothy K. Buennemeyer

> With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid—a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million information technology devices.[1]
>
> —Robert Gates, former US Secretary of Defense

The US Government has robust data networks that provide rapid transport of imagery, textual information, command and control data, and routine communications to support military operations and core business needs. This information is vital in the conduct of its war and peacetime missions. Historically, America's adversaries attempt to leverage network vulnerabilities to gain strategic advantage by exploiting information about US military and commercial activities, trade secrets, financial information, system architectures, and other data. The US is arguably the most interconnected nation on earth and it plays a hegemonic role with regard to establishing and maintaining the rules that govern the Internet. Americans embrace digital technologies that promise greater interconnection for governmental, corporate, and personal utility.

This article examines current Internet attack trends in the computer networking environment and proposes an enhanced framework for strategic system defense applicable to both corporate and federal networks. Presently, the balance of power favors those adversaries trying to attack US information systems, networks, and critical infrastructure. Well-designed cloud computing environments, however, may change the balance in favor of the defense, while reducing costs and improving service. The enhanced framework addresses these issues and assists in reducing the risks associated with assessing and adopting cloud computing.

Computing clouds are large data centers, filled with generic processing and storage facilities, and operated as multiple reconfigurable virtual servers.[2]

Colonel Timothy K. Buennemeyer, Ph.D., is a 2011 graduate of the US Army War College and winner of the Daniel M. Lewin Cyber-Terrorism Technology Writing Award. Currently, he is the Military Advisor for Net-Centric, Space, and Missile Defense Systems, working for the Director of Operational Test and Evaluation on the Secretary of Defense staff. He also teaches a graduate-level cybersecurity course for the Masters of Information Technology program at Virginia Tech.

Traditionally, cloud computing was represented by the outsourcing of an organization's computing infrastructure. Today, cloud computing presents "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[3]

Why Cloud Computing?

Emerging cloud computing technologies will subsume existing enterprise networks and encompass system defenses that are designed, implemented, and managed at corporate information technology (IT) processing centers. Once applications are logically extended through virtualization in a cloud computing environment, they are no longer tied to a physical location. The cloud service provider develops dispersed support and hosting facilities that allow applications to perform as needed. The system user merely needs to access the typically web-based application to run the desired program.

The trend for networking infrastructures and computing centers is shifting toward consolidation for cost savings. Cloud computing provides for the outsourcing of entire data centers, the saving of physical space, infrastructure, and labor costs. The prime benefit is the reduced cost of updating information systems and infrastructures, which is transferred to the cloud provider.[4] Cloud computing is a major evolutionary leap that virtualizes servers, infrastructures, and software as pay-for-use services. Government leaders have identified the benefits gained by adopting cloud computing, but they have not adequately considered the inherent risk with outsourcing IT.

Envisioning the future, the US Chief Information Officer (CIO) announced the Federal Data Center Consolidation Initiative and issued instructions for the Federal CIO Council to have governmental departments inventory their IT assets and integrate consolidation plans into their 2012 planning budgets.[5] The goal is to reduce IT costs, labor, energy, and physical space usage leading to the closing of 800 computing centers by 2015.[6] Based on this proposed migration, there is a critical need for an expanded defensive framework that includes an evolving cloud computing environment built on accepted network security principles. This expanded defensive framework would assist enterprise networking and cloud computing architects to design more secure systems.

Cloud service models describe IT design capabilities and levels of autonomy for customers. There are three accepted industry-wide cloud service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).[7] The initial capabilities migrating to cloud environments are electronic mail, content archiving, and vendor-provided SaaS applications. All benefit from consolidation into a virtualized cloud environment because these capabilities tend to require much lower processing cycles on servers.

There is, however, a migration paradox with various IT capabilities. Computational high-cycle-rate applications, transactional databases, and financial systems, mainly due to regulatory requirements, are ill-suited for cloud

computing. With SaaS and PaaS, the customer cannot alter the cloud environment. SaaS is the most restrictive of these models and only provides vendor-delivered applications for customer use, while PaaS permits customers to create programs using provided development tools and multiple coding languages.[8] IaaS allows customers to operate on-demand virtual hardware, load software, control firewalls, and adjust networking components.[9] Within this model, the cloud provider manages their physical servers; however, customers that employ their own applications in PaaS and their virtual servers in IaaS can maintain and secure the applications and virtual systems, respectively. The implication is that if an organization is already lacking in its security regime, then migrating to a cloud environment will not necessarily improve the overall security posture. Lastly, government and private sector budgets are shrinking, so IT and data security investments need to accomplish more with less. Adopting cloud computing is no panacea but it may assist in accomplishing these cost-saving efforts.

Cyberspace and Network Defense

Cyberspace is defined in Joint Publication 1-02 as "a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[10] Cyberspace is a contested domain, and the nation is "vulnerable to threats posed in cyberspace, while at the same time, dependent upon unfettered access."[11]

The Internet is proliferating around the globe, connecting diverse people in an expansive cyberworld. The combination of affordable IT and rapidly expanding interconnectivity is changing the way government, business, and individuals think, interact, and work. The networks provide the means to share information and make cyberspace, in a broader sense, a global commons for electronic information in the same fashion that the high seas provide the means to share commodities across a commons for maritime trade.[12] Like the sea, cyberspace is international and available for all to use. It is a shared resource that is loosely governed, routinely navigated via myriad uncharted routes, and, of increasing concern, often not well-secured.

As a new global commons, cyberspace is rapidly becoming a volatile, uncertain, complex, and ambiguous environment where governments, businesses, and individuals need to balance an information triad of confidentiality, availability, and integrity in order to establish a stable information security model. Confidentiality is the term used to describe preventing the disclosure of information to unauthorized individuals or systems. In information security, integrity means data cannot be modified undetectably.[13] For any information system to serve its purpose, data must be available when it is needed. This model is known as the CIA Triad of information assurance (IA), as shown in Figure 1.

Security models are critical in today's interconnected world, because information is routinely stored in data centers, providing continuous access at the speed of electronic transfer. At the basic architectural level, there are system hardware, software, and communications equities that must be protected. In

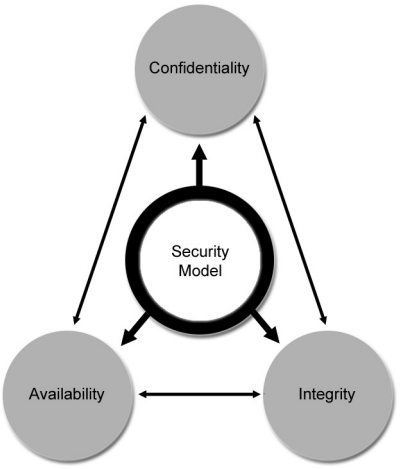

Figure 1. CIA Triad[14]

this security model, the triad's three design directions are often at the extremes and tradeoffs can potentially frustrate each other, so system designers endeavor to find equilibrium. Favoring any one design direction may compromise the integrity of the other triad pillars. This means for computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must function well and be in balance within the security model.[15]

DOD Directive 8500.01E establishes roles and responsibilities, procedures, and processes while defining the components of the CIA Triad.[16] IA is the means by which IT managers attempt to protect, maintain, and provide IT security for their organization through the training, testing, and monitoring of controls designed to secure an information resource.[17] IA offers measures that defend information by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation, while providing for restoration of information systems through the incorporation of protection, detection, and reaction capabilities.[18] With today's networks, IA measures are implemented through a Defense-in-Depth framework of layered security that extends from the originating network to the endpoint computer. These measures need to be expanded further to reduce risk more effectively in emerging cloud computing environments, while still addressing Internet attack vectors and vulnerabilities that may threaten the global information commons.

Framing the Strategic Environment of Cyberspace

Attacks in cyberspace are fast and can simultaneously target an individual or a broad spectrum of systems. Attackers are often anonymous with few concerns regarding attribution. The instantaneous nature and the ability to attack the entire domain simultaneously make cyberspace potentially a much more dangerous and vulnerable environment for the unprepared than the traditional warfighting domains.[19]

IT is crucial to every aspect of modern life, and a serious attack could cripple emergency services, defense networks, health care delivery, and power generation.[20] A cyber campaign would almost certainly be directed against the country's critical infrastructure, crossing boundaries between government and the private sector, and, if sophisticated and coordinated, could have an immediate impact along with delayed consequences.[21]

According to the US Computer Emergency Readiness Team, cyberthreats against the US are broadly categorized into five potentially overlapping groups: national governments, terrorists, industrial spies and organized crime

groups, hacktivists, and hackers.[22] Any of these groups can significantly impact US communication and System Control and Data Acquisition (SCADA) infrastructures. Of greatest concern are national-level cyberwarfare programs that pose threats along the entire spectrum of objectives capable of harming US interests.[23] Among the array of cyberthreats, only foreign government-sponsored programs are developing capabilities with the prospect of causing widespread, long-duration damage to US critical infrastructures.[24]

Traditional terrorist adversaries of the United States, despite their intentions to damage American interests, are less refined in their computer network capabilities and the ability to pursue cyber means rather than other adversaries.[25] They pose only a limited cyberthreat. The US should anticipate that substantial cyberthreats are possible in the future as a more technically competent generation of adversaries matures.[26] The majority of hackers do not have the motive or requisite tradecraft to threaten critical US networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated disruption causing serious damage, including the extensive destruction of property and loss of life. As the hacker population grows, so does the likelihood of a highly skilled and malicious hacker attempting and succeeding in such an attack.[27]

According to Symantec, the United States was the top-ranked country for malicious activity, accounting for 23 percent of all attacks, as shown in Table 1.[28] It is apparent from this report that malicious activity is also prevalent in the developed nations of the world, and attacks are capable of crossing all boundaries regardless of governmental, commercial, economic, and individual affiliation. The Internet is a permissive commons and as a consequence, so is its associated malicious actors, activities, and threats.

Rank	Country/Region	%	Malicious Code Rank	Spam Zombies Rank	Phishing Website Hosts Rank	Bots Rank	Attack Origin Rank
1	United States	23	1	3	1	2	1
2	Brazil	6	6	2	10	3	3
3	India	6	2	1	30	20	8
4	Germany	5	11	5	3	4	7
5	China	4	3	28	7	6	2
6	United Kingdom	4	4	7	4	9	4
7	Taiwan	4	23	12	15	1	9
8	Italy	4	21	11	11	5	6
9	Russia	3	15	9	8	16	5
10	Canada	3	8	41	2	17	12

Table 1. Malicious Activity by Country and Region[29]

While nonstate sponsored computer network exploitation poses a serious risk to US national security, those exploits are less troubling when compared to a nation-state threat, such as that of China, which seeks to go beyond cyber espionage in order to achieve military effects in cyberspace.[30] Specific information regarding attacks against US Government networks and attribution is classified, so only representative open-source information is available, as in Table 1. From the discussion of SCADA attacks, one can surmise military effects, such as a shutdown of regional power generation systems and the susceptibility of distribution networks to data theft, are all plausible examples of the broad range of possible threats. As IT becomes increasingly integrated into every facet of American life, US national security planners view its pervasiveness as a target and weapon; it is the one critical component on which modern societies depend, a dependence not lost on potential enemies.[31]

The US Government identified the IT sector as an area of the nation's critical infrastructure and aligned its protection under the Department of Homeland Security (DHS) in 2009.[32] According to the National Academy of Engineering, cybersystems are the weakest link in our national security.[33] Many of these vulnerabilities are directly linked to the SCADA systems that manage critical utilities—electrical grids, water supplies, sewer flows, and gas transmissions—across America. Older SCADA systems incorporated limited security and operated on closed communication systems, but most modern SCADA systems use the Internet to pass information.[34] Thus, SCADA systems are exposed to asymmetrical attacks.[35] SCADA attacks pose a critical threat, because direct control of these systems could create the potential for large-scale power outages or man-made environmental disasters.[36] It is estimated that for every 24 hours of SCADA down time from a major attack there would be $6.3 million in damages with the greatest costs in the oil and gas sectors.[37]

Over the years, various commissions have examined cybersecurity, focusing their efforts on SCADA systems, communications, financial networks, and other network-enabled infrastructures. Reports from these efforts conclude US critical infrastructures are increasingly dependent on information and communication systems, and this dependence is a growing source of vulnerabilities.[38] Presidential Executive Order 13286 required the United States to protect against "disruption of the operation of information systems for critical infrastructure and help to protect the people, economy, essential human and government services, and national security of the US, and to ensure any disruptions that in fact occur are infrequent, of minimal duration, manageable, and cause the least damage possible."[39]

Dennis Blair, former Director of National Intelligence, stated, "the cyber criminal sector, in particular, has displayed remarkable technical innovation with an agility presently exceeding the response capability of network defenders . . . . Criminals are collaborating globally and exchanging tools and expertise to circumvent defensive efforts, which makes it increasingly difficult for network defenders and law enforcement to detect and disrupt malicious activities."[40] Internet-related economic losses reached $42 billion in the United States and

$140 billion worldwide in 2008, while globally, companies may have lost over $1 trillion worth of intellectual property due to data theft.[41] Stolen trade secrets and proprietary research, lost royalties, patent infringements, and leaked financial information comprise a growing list of data lost in Internet-related thefts.

The security firm McAfee surveyed over 1,000 businesses regarding possible data loss. Their survey has national security implications; its results indicate substantial amounts of vital information, such as intellectual property and sensitive customer data, transferred between companies and continents are being lost.[42] The report concludes that companies lost on average $4.6 million worth of intellectual property in 2008.[43] It is difficult to evaluate the total financial losses to businesses because companies are reluctant to report figures due to concerns over losing consumer confidence. It costs an average of $600,000 per firm to respond to each security breach involving the loss of information. This figure only reflects the reported cleanup costs, legal fees, and victim notifications; it does not include the infrastructure costs associated with prevention and detection.[44] McAfee's research further revealed that respondents worried far more about their company's reputation due to public relations damages and information leakage than they did about the financial impact.[45] Thus, an examination of defensive capabilities to protect US cyberspace is necessary.

Network Defense Options in a Cloud Computing Environment

Network defenses may be classic or modern. Figure 2 presents the classic security "onion" diagram employed in traditional IT environments. It focuses on the physical, procedural, technical, and personnel security that impact the core IT components of data, applications, hosts, and networks.

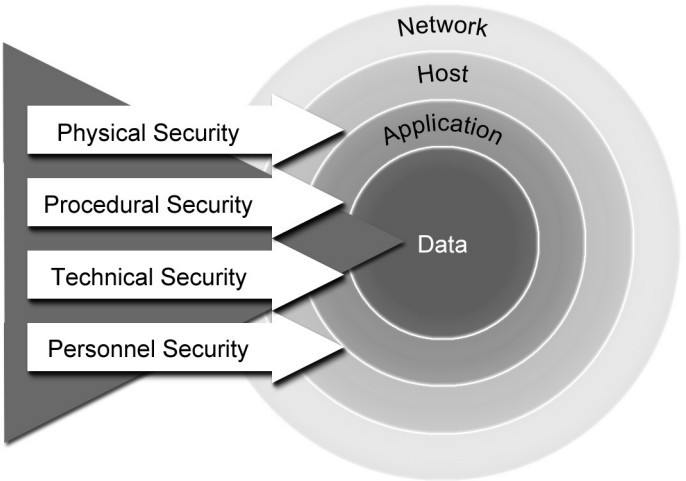

Figure 2. Classic IT Security "Onion"

Over time, more robust defensive constructs evolved to better protect information, servers, systems, and transport communications. As newer

capabilities emerge, defensive technologies adapt. Previously, technology companies fielded new capabilities into the marketplace as rapidly as possible with security measures following as an afterthought. This strategy frequently left security gaps in organizational computing environments. In today's environment, security is a basic design consideration when systems are first proposed, and technologies lacking these defensible capabilities are doomed. A modern information security construct is outlined in Figure 3. While this security construct is not all inclusive, it is representative of the defense-in-depth concept that will continue to evolve as new capabilities and mediums enter cyberspace.[46]

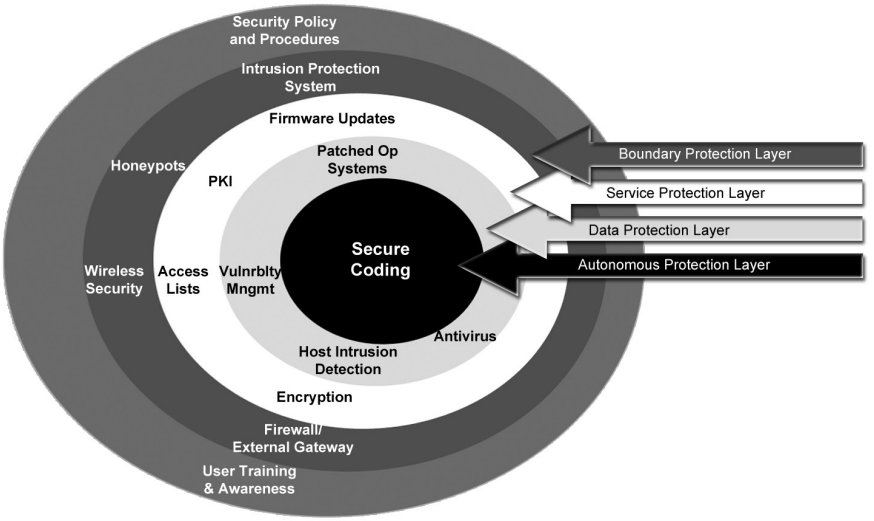

Figure 3. Modern Layered IT Defense Adapted from DHS Cyber Defense Strategy[47]

Bearing in mind both classic and modern network security defenses, it should be pointed out that simply migrating an organization's IT capabilities to a cloud environment does not abdicate the data owner's security responsibilities. Cloud computing does not change the existing defensive means available to security specialists. In truth, the center of gravity in cloud computing is the physical servers, and their protection is paramount. If physical servers are compromised, then the hosted computers will likely be compromised. This places a heightened focus on the provider's abilities to protect the physical servers. Statistics indicate one-third of breaches result from lost or stolen laptop computers and employees accidentally exposing data on the Internet; nearly 16 percent of breaches are due to insider theft.[48] When a user logs out from cloud computing services, the browser can be set to flush automatically, leaving nothing of value on the remote computer. Security concerns with cloud computing are more a cultural issue associated with outsourcing rather than any proven design weakness.[49]

Cloud Computing Network Defense Examination

Due to ever expanding US interests, a strategic cybersecurity framework for cloud computing should be developed to shape protection efforts for US cyber infrastructure, communication systems, and commercial, financial, and military networks, protecting them from a wide range of crippling attacks and exploitive threats. Failure to protect governmental, military, and commercial networks can lead to the loss of intellectual property, trade secrets, and much more. The compromise of these crucial networks would create chaos in the banking, governmental, and military sectors.

Securing networks with a physical infrastructure presents known system environments to defend. Cloud environments require additional risk consideration because the capabilities, data, and software are virtualized, while the physical infrastructure is outsourced and may reside outside the governance laws of a particular country. Traditional network security frameworks, such as the defense-in-depth approach, are applied to fixed networks to secure physical IT environments; however, this approach may not be adequate for cloud computing environments because systems are virtual and potentially mobile. Additionally, networking's instantaneous nature and adversaries' ability to attack the entire cyber domain make cloud computing potentially vulnerable.[50]

Physical and virtual borders are critical because cloud providers select their sites based on economic, connectivity, power availability, and security criteria, and they often have to make special arrangements between countries regarding data movement restrictions.[51] A growing number of people believe cloud computing represents a paradigm shift on par with the development of mainframes, personal computing, client-server computing, and the Internet.[52] System owners are generally risk adverse, so adopting cloud computing as a solution requires a comprehensive defensive framework in an effort to ensure security. While cloud services are being used, experts cite security, interoperability, and portability as major challenges to further adoption.[53] Conversely, senior IT leader expectation is for enabling cost savings while increasing the ability to quickly create and deploy enterprise applications.[54] This is where current policy and subsequent security framework are lacking. Working with agencies, industry, and academe to correct this lack of security, the National Institute of Standards and Technology is leading the development of standards related to security, interoperability, and portability for the US CIO.[55] The expectation is the development and fielding of well-defined standards capable of shortening the adoption cycle, enabling cost savings, and increasing the ability to deploy enterprise applications. Additionally, a government-wide risk and authorization program for cloud computing will permit agencies to use the authorization by another agency with the objective of driving a set of common services across the government supported by the entire community, rather than an agency-specific risk model.[56] This effort is critical because it will reduce the burden in the performance of IA certification and accreditation of applications and systems, resulting in greater cost efficiency.

Network State-of-the-Art Risk Framework

Industry-wide IA best business practices and computer defensive measures are not uniformly implemented, so a framework is necessary to assist with prioritizing and coordinating these defensive efforts. Cybersecurity is not just about deploying specific technologies to counter risks, as such; an effective security program for any organization will depend on its willingness to accept security as a constant constraint on all cyber activities.[57] The critical aspect for cloud environments is to understand what the new and inherent risks are and how this change in service delivery might be affected. Risk assessments are a cornerstone in defining, understanding, and planning remediation efforts against various threats, potential vulnerabilities, and architectural design flaws.[58] The establishment of an enhanced defensive framework for cloud environments is only prudent. According to the DHS, a defense-in-depth framework at a minimum should include:

- Know the security risks that an organization faces.
- Quantify and qualify risks.
- Use key resources to mitigate security risks.
- Define each resource's core competency and identify any overlapping areas.
- Abide by existing or emerging security standards for specific controls.
- Create and customize specific controls that are unique to an organization.[59]

Understanding a framework is a guide for assessing risk—this framework provides a valuable starting point. In a traditional layered defensive construct, the systems tend to be collocated in relatively close proximity within an area processing center, often managed by the data owner.

The challenge of increasing security to cloud computing is twofold. First, the owner's data and systems are often outsourced to an external cloud environment provider, so the owner no longer sets the environment's security policy or maintains its security posture. Second, cloud environments are established and interconnected in multiple locations. Their physical servers are often located in geographical areas where expenses in terms of labor and governmental regulation are minimal.

There are hidden drawbacks nested amongst the benefits of entering into a cloud environment. For example, an organization may benefit through the reduction of technical staff, which can free up labor and capital. However, governance of the cloud environment is not transparent, so the data owner may unknowingly inherit higher risk for intrusion from the provider. Once an organization outsources its technical support, it is difficult to reestablish organic technical skill sets. Simply stated, it takes years to develop institutional knowledge and then apply that knowledge to technical solutions. Cost savings is often the driving force for adopting cloud computing. The technical benefits are scalability and flexibility that permit an organization to pay for cloud computing resources as required. One example comes from the private sector, when one cloud environment allowed for increased response capability as demand jumped from 25,000 to more than 250,000 users in less than a

week.[60] Because of cloud computing, the company was able to scale from 50 to 4,000 virtual machines in three days to support this increased demand.[61] This capability would take significantly longer under the government and military's current construct, so the adoption of cloud computing comes down to costs, technical staff capabilities, risks, and benefits. All these factors need to be carefully weighed when making the decision to migrate to cloud computing.

State-of-the-Art Risk Framework for Cloud Computing

Along with the tendency for cloud environment outsourcing, this article proposes adding five additional areas to the existing defense-in-depth framework. Below are the proposed areas:

- Assess the security posture of the cloud environment.
- Know the physical location of the actual cloud computing center(s).
- Understand your service-level expectation relative to perceived risks.
- Assess applicable governance, laws, regulations and policies.
- Know your tolerance for service interruption, data loss, and recovery.

With these additional framework layers, organizations will be better able to assess their information security posture. Having an accurate and well-documented architecture and complementary risk assessment enables an organization to be more security conscious, deploy effective threat countermeasures, and be equipped to recognize and understand security incidents more readily.[62] Through cloud computing, the service provider establishes cloud architecture, security posture, and provides the service delivery. It is incumbent on the service and data owner to fully appreciate and assess all environmental risks.

Applicability for Federal Enterprise Environments

The DOD operates one of the largest and most robust enterprise computing environments in the world. Although the DOD's network structure is linked, the military services typically operate distinct domains, so it will require a major financial and labor initiative to migrate to a cloud environment. This consolidation effort will cause the military departments to examine IT investments from a Title 10 perspective, possibly limiting their autonomy with regard to their individual mandates to man, equip, and outfit their forces. Migration to a cloud environment will likely occur incrementally over the next 5-10 years and could allow for the recapitalization of hundreds of millions of dollars in network operating funds. As shown in Table 2, the DOD currently spends over $36.3 billion annually for IT.[63]

Bureau	Total FY2011 Spending (Billions)	No. of Total Investments
Department of the Army	$7.3	256
Department of the Air Force	$6.8	651
Department of the Navy	$7.6	789
Department of Defense Agencies	$14.6	536
Department of Defense (Total)	**$36.3**	**2,232**

Table 2. DOD IT Portfolio Budget for FY2011[64]

The government, as part of a broader IT transformation, needs to fundamentally shift its mindset from building custom systems to adopting light computing technologies and utilizing shared cloud solutions.[65] This shift is absolutely necessary because the various departments typically build systems that duplicate capabilities and lack integration, causing unnecessary IT redundancies and increased costs. The explosion in the number of federal data centers from 432 in 1998 to 2,094 in 2010 highlights the rapidity of this ongoing IT expansion.[66] With a subjective examination of the DOD IT expenditures juxtaposed across the Federal Government, one can sense the potential cost savings in the billions of dollars simply by eliminating IT redundancies, consolidating server farms and data centers into cloud environments, and reducing technical staff.

Information services should enable the government to better serve the American people. Despite spending more than $600 billion on IT over the past decade, the government has achieved little in terms of the productivity improvements as compared to the private sector.[67] This growth alone reflects federal employees' ever-increasing dependency on IT. Unless checked by a transition to cloud computing, this IT growth trend will persist and expand. The National Security Agency is trimming its allocation to IA from $915 million in 2010 to $902 million in 2011.[68] It is likely this trend of reducing expenditures for IT security will continue across the government as budgets tighten.

IT projects often run over budget, fall behind schedule, or fail to deliver promised functionality, because the project designer's approach simply aims to deliver full functionality against a specific suspense, rather than modularizing projects into more manageable chunks and demanding new functionality at established time periods.[69] This progress is further complicated by a reliance on proprietary application and system design, something cloud solutions might resolve. This new way of designing systems amounts to a major change in mindset as well as an adjustment to the key functions of management and staffing. If cloud computing is the next generation environment, then the technical staff will require extensive training. Although there will likely be reductions in technical staffing areas, such as system administrators, network monitoring personnel, and router and gateway administrators, there is a probability for increases in application and data developers. It is a fact that experienced technical staff often help translate organizational missions and visions into complex multimedia presentations, using integrated IT

capabilities. Thus, the loss of these experienced IT staff members may result in a reduction of organizational effectiveness.

Conclusion

Research has revealed the challenges associated with providing network defense in the current enterprise environment and recognized that consolidating area processing centers into cloud environments is the likely future migration path. The primary reasons for adopting a cloud environment are rapid scalability and flexibility with SaaS, PaaS, and IaaS. There is a perception that migrating to cloud computing will also yield cost savings through reduced physical infrastructure and technical staff. While a cloud environment may significantly reduce physical infrastructure requirements, it may not significantly reduce staffing requirements as departments would still require technical staff to maintain the virtual servers and manage data.

Additionally, this article proposed an enhanced defensive framework to better assess the risks of cloud computing. While the existing framework is valuable, the added assessment areas address the dynamic nature of cloud computing and afford the system owner improved attack risk mitigation through a more complete assessment of the environment.

The 2010 Joint Operating Environment predicts network connectivity will grow by 50 percent a year, providing 100,000 times more bandwidth in 2030 than today; and computers will run one million times faster. If these predictions become reality, a home computer would be capable of downloading the entire Library of Congress in 128 seconds.[70] With these predictions in mind, it is almost a certainty that security challenges and the sophistication of attacks will increase proportionately. The greatest concern for government and businesses is being lulled into a false sense of security by migration to cloud environments. The benefits of such a migration are equally apparent, but the consolidation of multiple virtual machines into an outsourced cloud computing environment will incur an undeniable risk. Ultimately, such decisions come down to data owner cost and risk considerations, expectations, and the ability to accept not having complete control of their systems.

With commitment, careful planning, and systematic implementation, those designing the defense need to incorporate cyberspace's virtual world if there is to be any chance of limiting damage in the real world.[71] The defense of virtual computers is more akin to holding atmosphere in your hand or cyberspace as the case may be. Clausewitz stated, "The defender is at greatest disadvantage when compelled to protect a wide area against multiple axes of advance. In this instance, the attacker using surprise may throw his full strength at any one point."[72] Conclusively, the network defense employs a substantially greater means by which to preserve security in computing environments. This fact may result in the attacker actually having the initiative and an asymmetric advantage in cyberspace. Well-designed cloud computing environments, however, may provide an opportunity to change the balance back in favor of the defense, while reducing costs and improving service.

Notes

1. U.S. Secretary of Defense Robert M. Gates, *Submitted Statement to Senate Armed Services Committee* (Washington, DC: US Senate), January 27, 2009, 8.
2. Clive Davidson, "Cloud Control," *Risk* 23, no. 10 (October 2010): 70, in ProQuest (accessed November 22, 2010).
3. U.S. Department of Commerce, National Institute of Standards and Technology, *The NIST Definition of Cloud Computing (Draft)*, Special Publication 800-145 (Draft), (Washington, DC: U.S. Department of Commerce, January 2011), 2.
4. Davidson, "Cloud Control," 71.
5. U.S. Chief Information Officer Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, DC: The White House, December 9, 2010), 5.
6. Ibid.
7. Mike Gray, ""Cloud Computing: Demystifying IaaS, PaaS, and SaaS," *ZDNET*, October, 21, 2010, http://www.zdnet.com/news/cloud-computing-demystifying-iaas-paas-and-saas/477238 (accessed April 19, 2011).
8. SP 800-145, 2.
9. Gray, "Cloud Computing: Demystifying IaaS, PaaS, and SaaS."
10. U.S. Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: U.S. Department of Defense, April 12, 2001 amended through September 30, 2010), 126.
11. William T. Lord, "Cyberspace Operations: Air Force Space Command Takes the Lead," *High Frontier* 5, no. 3 (May 2009): 3.
12. Arthur K. Cebrowski, "Transformation and the Changing Character of War?," *Transformation Trends*, June 17, 2004, http://www.hsdl.org/?view&did=448180 (accessed January 5, 2012).
13. Chad Perrin, "The CIA Triad," June 30, 2008, (Louisville, KY: TechRepublic), http://www.techrepublic.com/blog/security/the-cia-triad/488 (accessed January 23, 2011).
14. Cisco Learning Network, "What is the CIA Triad," https://learningnetwork.cisco.com/message/59995 (accessed November 19, 2010).
15. Perrin, "The CIA Triad."
16. U.S. Department of Defense, *Information Assurance*, DOD Directive 8500.01E, (Washington, DC: U.S. Department of the Army, October 24, 2002, Certified Current April 23, 2007), 4.
17. U.S. Department of the Army, *Information Assurance*, Army Regulation 25-2 (Washington, DC: U.S. Department of the Army, March 23, 2009), 1.
18. U.S. Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, 175.
19. David M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Forces Quarterly* 58 (Third Quarter, July 2010): 49.
20. Andrew Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," *SANS Institute InfoSec Reading Room*, February 23, 2005, (Bethesda, MD: SANS Institute), 5, www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644 (accessed November 19, 2010).
21. Timothy Shimeall, "Countering Cyber War," *NATO Review* 49, no. 4 (Winter 2001): 17.
22. United States Computer Emergency Readiness Team, Control Systems Security Program (CSSP), "Cyber Threat Source Descriptions," http://www.us-cert.gov/control_systems/csthreats.html (accessed January 3, 2011).
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid.
27. Ibid.

28. Symantec Intelligence Quarterly Report for July–September 2010 (Mountain View, CA: Symantec, 2010), 6, http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_ intelligence_qtrly_july_to_sept_WP_21157366.en-us.pdf (accessed December 15, 2010).

29. Ibid.

30. Brian M. Mazanec, "The Art of Cyber War," *Journal of International Security Affairs*, no. 16 (Spring 2009): 84.

31. Shimeall, "Countering Cyber War," 16.

32. Jeffrey L. Caton, "Cyberspace and Cyber Operations," *Information Operations Primer*, AY11 ed., (Carlisle, PA: US Army War College, November 2010), 21.

33. S. Massoud Amin, "Securing the Electricity Grid," *National Academy of Engineering*, http://www.nae.edu/ Publications/Bridge/TheElectricityGrid/18868.aspx (accessed January 3, 2011).

34. Caton, "Cyberspace and Cyber Operations," 20.

35. Amin, "Securing the Electricity Grid."

36. Stewart Baker, Shaun Waterman, and George Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (Santa Clara, CA: McAfee, 2011), 9, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf (accessed January 5, 2012).

37. Ibid., 10.

38. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," 5.

39. George W. Bush, *Presidential Executive Order 13286 amending 13231 Critical Information Protection in the Information Age* (Washington, DC: The White House, February 28, 2003).

40. U.S. Director of National Intelligence Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Washington, DC: US Senate, February 2, 2010), 4.

41. Ibid., 40.

42. McAfee, *Unsecured Economies: Protecting Vital Information* (Santa Clara: McAfee, 2009), 3, http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf (accessed January 5, 2012).

43. Ibid.

44. Ibid., 7.

45. Ibid.

46. U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* (Washington, DC: U.S. Department of Homeland Security, October 2009), 14.

47. Ibid.

48. Elinor Mills, "Cloud Computing Security Forecast: Clear Skies," *CNET News*, January 27, 2009, http://news.cnet.com/8301-1009_3-10150569-83.html (accessed January 26, 2011).

49. Ibid.

50. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," 49.

51. Davidson, "Cloud Control," 72.

52. Ibid., 73.

53. U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 7.

54. Ibid.

55. Ibid.

56. Ibid., 8.

57. U.S. Department of Homeland Security, *Recommended Practice*, 14.

58. Ibid., 15.

59. Ibid.

60. U.S. Chief Information Officer, *25 Point Implementation Plan*, 6.

61. Ibid.

62. U.S. Department of Homeland Security, *Recommended Practice*, 29.

63. U.S. Office of Management and Budget, "IT Dashboard," http://it.usaspending.gov/ (accessed January 27, 2011).

64. Ibid.

65. U.S. Chief Information Officer, *25 Point Implementation Plan*, 3.

66. Ibid.

67. Ibid., 1.

68. J. Nicholas Hoover, "NSA Details Information Assurance Spending," *InformationWeek*, April 9, 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml? articleID=224202447 (accessed January 27, 2011).

69. U.S. Chief Information Officer, *25 Point Implementation Plan*, 1.

70. US Joint Forces Command, *Joint Operating Environment* (Suffolk, VA: U.S. Joint Forces Command, February 18, 2010), 36.

71. Shimeall, "Countering Cyber War," 18.

72. Carl von Clausewitz, *On War*, trans. Michael E. Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 364.