# The Active Shooter System

**LTC Phillip G. Burns, U.S. Army**

**Abstract.** The proposed Logical Active Shooter System is a referential architecture that guides the securing of data as DoD migrates to a Joint Information Environment. The goal is to secure critical information from malicious access or misuse that impacts mission accomplishment throughout the Joint phases of operation.

## Introduction

The United States of America faces a challenge—cyber threats to national interests abound, while homegrown security professionals who are able to operate effectively in cyberspace do not. By all accounts, this lack of effective personnel is the weakest area in building and defending the network. A study by Frost and Sullivan supports this assertion [1]. To add to this, many of today's cybersecurity professionals have to read up on cyber threats, as many of them are digital immigrants and are not digital natives. In contrast, digital natives grew up with computers, video games and computer graphics. Automation is second nature to digital natives.

DoD organizations, such as U.S. Cyber Command (USCYBERCOM) and the NSA, must reach out to digital natives, recruiting and molding them to build, defend the military network and, at times, hunt for malicious intruders set on attacking the network. Of course, distinctions between United States Code (USC) Title 10 and USC Title 50 [2]—between operations and intelligence—may constrain how we build and defend the network, as well as hunting adversaries. According to one researcher, decisions to execute a defense against a cyber attack are often measured in seconds or milliseconds [3]. Operators placed in that position must have Title 10/50 authorities and the ability to make decisions locally, to apply operational effects necessary to protect or isolate the network. This decision making is a learned skill that adds to the challenge discussed at the outset.

As USCYBERCOM and NSA focus on building the bench of cybersecurity professionals, measures must be in place to protect information as the gap decreases between digital natives and digital immigrants. Until the bench is built, the focus must be to secure data, but not overly restrict the DoD users' access to data in a manner that prevents collaboration.

Within the scope of this discussion, the DoD is directing the consolidation of disparate data centers across the DoD network to a select set of core data centers. Efforts will lead to the integration of the Army's portion of the DoD network with the Joint Information Environment (JIE) at Figure 1. The JIE will provide a single network that is secure, standards-based, flexible and supports versatile mission sets [4].

Future Army network capabilities include chat services and software defined radios that, in accordance with the Unified Compliance Framework, will connect users at home or work with deployed enterprise users. As Figure 1 indicates, all is geared to ensure enterprise users have the "…information they need, when they need it, in any environment, to manage the Army Enterprise and enable Full-Spectrum Operations with our Joint, Coalition, and Interagency partners [5]." JIE will usher unprecedented access to information and a new era of collaboration and situational awareness that enables Mission Command, presenting a formidable foe to the Nation's enemies, with the technology and a network to back up its teeth.

While JIE will provide the standards and the common environment, the Services will employ technologies, such as Host Based Security System (HBSS), Public Key Infrastructure (PKI), Rights and Identity Management, to assure confidentiality, integrity and availability of information; however, these technologies alone may not foster a completely secure environment. The Deployed Environment and Defense Information Systems Network (DISN) clouds at Figure 1 typify one-to-many user interactions, which is hard to audit but not impossible.

This article focuses on logically and physically securing critical DoD information with limited impact to the user's experience and collaborative efforts to ensure situational awareness critical to Mission Command. This article explores a "Logical Active Shooter System" that ensures data is protected from unintentional or intentional spillage. The system must support Title 10/50 requirements, while simultaneous restricting the digital natives' ability to circumvent its controls. The Bradley Manning incident (i.e., "Wikileaks") is mentioned as a use case.

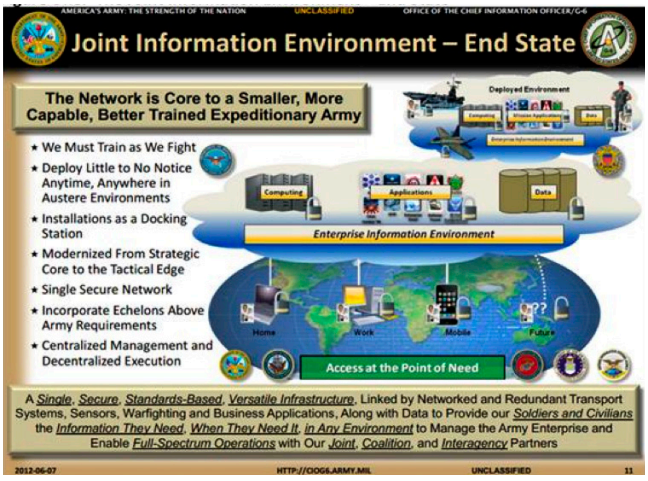



Figure 1. The Joint Information Environment – End State

## The Logical Active Shooter System

U.S. Army Mission Command Center of Excellence's (CoE's) Requirement Governance Team, in coordination with U.S. Army Signal CoE's TRADOC Capability Manager for Global Network Enterprise, are developing an operational framework for a cloud-based computing network. Figure 2 illustrates [6] a proposed operational view underpinning the principles of this cloud-based computing network. Deployment of the Logical Active Shooter System would occur after the JIE end state as illustrated in Figure 1.

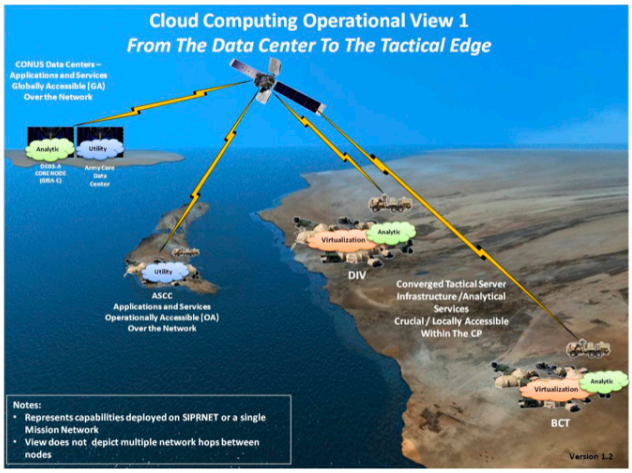



Figure 2. Cloud Computing Operational View

Security technologies, such as HBSS, PKI, and Rights and Identity Management, will be critical to the future network and engineered in the architecture from the start to ensure the end state of a "Single Secure Network." The DoD and Army cloud-based computing networks will leverage the NIST definition of cloud computing: "…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 [7]." The NIST definition implies that anonymous access to information is expected; however, shared concerns of mission security requirements, policy, and compliance considerations will be factored into instantiations of a cloud-based computing environment.

Within a deployed setting, loss of data or spillage of classified material is a real concern, and anonymous access is hard to monitor. It takes leadership and active participation of users to enable an environment where mission critical information is secured from unauthorized users and access.

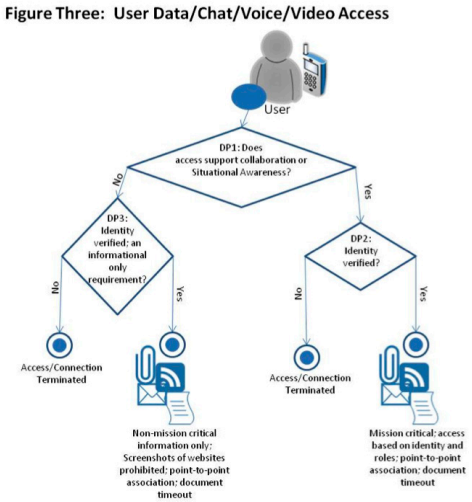
The Bradley Manning incident illustrates the complexity of preventing the spillage of classified material. The Bradley Manning incident is an excellent use case, as it serves as a stark reminder when lax involvement and security posture by leadership and users go awry. For uninitiated readers, Bradley Manning, a digital native who represented a class of insider threat (a disgruntled employee who displays some emotional distress), pled guilty to mishandling classified materials and uploading said information to WikiLeaks.org via his personal laptop. One researcher noted that to mitigate situations like this, "[a]n 'active shooter'-like stance or posture is needed. Technical controls are required and in some cases are implemented, but to what degrees of success are debatable [8]." The researcher goes on to note that, "Involvement of leadership helps to improve IT security, and a well-informed IT security staff helps to identify and correct situations [9]." (For the purpose of this article, taking an "active shooter"-like stance is to intercept the malicious attacker while he or she is in the progress of executing the attack on the network or information system. This taking action can be via involvement of leadership/fellow users or automated enforcement of rules and roles.)

Taking an "active shooter"-like stance alone will not in itself adequately protect the DoD network and mission critical information, because the distributed and open-access nature of cloud computing injects a level of risk that must be factored into risk assessments and technical controls. A roles- and rules-based system is needed to adjudicate or restrict access. Figure 3 illustrates a recommended capability that can secure critical information and logically establish an "active shooter" capability. For the purpose of this article, critical information is defined as information that enables situational awareness within a mission setting that includes classified or For Official Use Only information where its unintended release or leakage impacts a mission or strategic aims. Information releasable to the public is not defined as critical information that will be protected.

The first step is to adjudicate access based upon established roles- and rules-based policies, to which users can authenticate through technology such as Rights Management or PKI. The goal is to marry roles- and rules-based access to the specific platform where access was initially generated. This would be a goal at end state. This is decision point #1 (DP1) as illustrated in Figure 3. If access to information enables collaboration in support of mission informational and situational awareness requirements, then DP2 is enabled. If identity is not verified, then access to information is terminated. Levels of access to information under DP2 are determined by roles- and rules-based access requirements. Information can be in the form of voice, video, and data. Access to data files is time-limited and files are automatically shredded to keep information relevant and current. Timeframes for access to data file are determined by the data owners.

If the answer to DP1 is no, then DP3 is enacted, and the user's identity is verified. If the user's identity is verified, then the user has access to non-mission critical information only; screenshots of websites are prohibited; and data files are set to time out to ensure information is relevant and current. If the user's access under DP3 cannot be verified, then access to information under this category is terminated.

Figure 3. User Data/Chat/Voice/Video Access



As Figure 3 represents a recommended capability, there are several technologies that can enable the capability represented is Figure 3. While there are a number of solutions available, this article will discuss two: 1) Narus N10 and 2) Adobe's document security solution.

(For the purpose of this article, Narus N10 and Adobe's document security solutions represent desired characteristics critical to securing critical information as defined above, which includes lifecycle management of critical documents. The narrow scope of solution sets supports refinement of critical characteristics of the Logical Active Shooter System: role- and rule-based access; a virtual workplace where documents are shredded, encrypted, and interleaved upon termination of connection to the virtual workplace; supports bandwidth constrained environment.)

The first solution is the Narus N10. As a primer, Narus is a wholly owned subsidiary of Boeing. The N10 has the ability to authenticate access and contain access based upon roles and established rules. Updated information is continuously rendered to the user, and a dynamic auditing capability is enabled to scope future access based upon the informational needs of the user. Users do not directly access secured material. Users request access to a particular document and a secured, virtual workplace is created via a protected tunnel (see Figure 4). This virtual workplace facilitates tracking, queuing, and securing of document requests. In addition, the Narus N10 interfaces with a Mobile Synchronization Module, with which users can access current information every time documents are introduced to their workplace.

According to Narus, the N10 ensures that "[d]ocuments stored in the repository are shredded, encrypted, and interleaved with white noise before being scattered randomly throughout the storage environment [10]." Narus further touts that uploaded documents cease to exist in any "integral form" and, therefore, present no target for hackers to attack [11].

The second solution is Adobe's suite of document security software. Adobe's document security solutions support data encryption with symmetric, asymmetric, or hybrid keys, in order to ensure confidentiality. Adobe's solution supports IT security professionals or system administrators to set permissions, as well as support dynamic document control, expiration, and digital signatures. Adobe's document security product line includes Adobe Acrobat Family, Adobe Reader, Adobe LiveCycle Reader Extensions, Adobe LiveCycle Digital Signatures, and Adobe LiveCycle Rights Management [12]. Because Adobe supports integration with Lightweight Directory Access Protocol and Active Directory, roles- and rules-based access control is possible.

While Adobe can secure information in accordance with Figure 3, its products only secure the .pdf file type, and not the full breadth of file types in use across the DoD enterprise. In contrast, Narus N10 supports more of the file types found on the DoD Enterprise. Narus N10 may also have application in securing sensitive information on strategic networks; however, before use in a tactical setting, it must first be evaluated, as tactical users often access information within a bandwidth constrained environment.

While one goal of the JIE is to eventually virtualize Joint common services, tactical users must have access to critical information even while not connected to the DISN. Therefore, developing and maintaining a common operating picture in a disconnected environment is critical to the Warfighter and the Commander on the ground. Situational awareness data and collaborative services in support of missions must go unfettered throughout the Joint phases of the operation. Selected capabilities must support this critical need in addition to securing critical information from malicious exfiltration or willful disclosure of critical information.

In consideration of the Narus and Adobe capabilities, access validation through Rights Management, PKI, and Active Directory is a critical enabler to DP1. DP2 is divided into two sequels: DP2-A and DP2-B. DP2-A supports users in a bandwidth constrained environment, or users who will be adversely impacted if disconnected from the DISN. Therefore, DP2-A provides access to mission critical information with point-to-point association and document timeout to ensure information is current. DP2-B will support user's access to critical information when bandwidth and potential disconnection from the DISN is

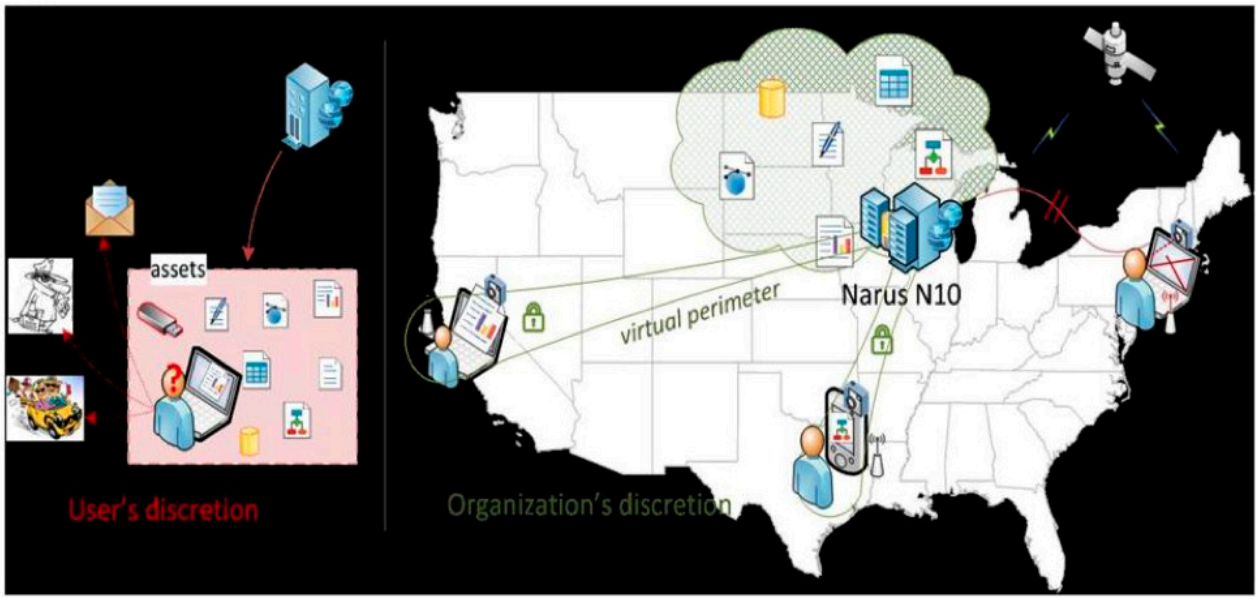



Figure 4. Narus N10

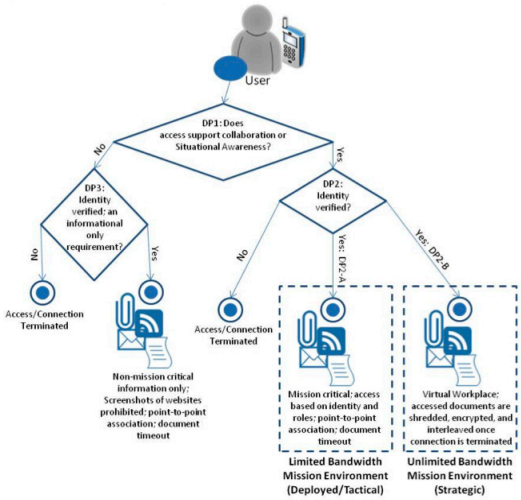



Figure 5. User Chat/Chat/Voice/Video Access

not an overarching concern. DP2-B provides a virtual workplace that facilitates access to mission critical information, in a manner similar to the Narus N10 capability mention above. Figure 5 provides an updated view of the proposed Logical Active Shooter System.

## Conclusion

The two Logical Active Shooter System solutions described in this article are only the tip of the iceberg of capabilities that DoD can leverage. They provide a referential architecture that can support a secure cloud-based network. Both capabilities can go far to mitigate an insider threat like Bradley Manning. With the recent posturing and alleged hacking exploits by the Democratic People's Republic of Korea, the need to secure information against all threats becomes paramount as we develop and migrate to a Joint Information Environment. If an organization takes an appropriate "active shooter"-like stance, then the insider threat (intentional or unintentional) can be effectively mitigated. A logical means of bolstering this "active shooter"-like stance is needed to secure critical information and limit exploitation of critical information by insider and outsider threats.

## Additional Reading

1. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action" by Mr. Andru Wall, which can be found at <http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Wall1.pdf>. Mr. Wall is a former legal advisor for U.S. Special Operations Command Central (2007-2009). He provides a thorough synopsis of the Secretary of Defense's unique Title 10/50 responsibilities, as they pertain to unconventional and cyber threats. Within the document, Title 10/50 decisions in response to cyber threats are made in milliseconds and often by the same individual.

2. "Data Breach Investigations Report 2012" by Verizon's RISK Team, with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and the United States Secret Service. It can be found at <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf>. The report provides statistical analysis of compromised records, and provides a analysis of cyber threats resulting in the compromise of records.

3. "NSA: Looking for a Few Good Cybersecurity Professionals" by Dirk Smith, which can be found at <http://www.networkworld.com/news/2012/111312-nsa-cybersecurity-264223.html>. Within the article, the reader is made aware of a current shortfall of 20,000 cybersecurity professionals, with a projected shortfall of 40,000. No concrete date was given for the aforementioned prediction. NSA is attempting to mitigate this by partnering with the Nation's service academies, colleges, and universities.

## ABOUT THE AUTHOR

LTC Phillip G. Burns is a capability manager for the U.S. Army Signal Center of Excellence. Prior to that, he served as the Information Assurance Officer for the 2nd Infantry Division, Camp Red Cloud, South Korea. He holds a Master of Science in Computer Information Systems. In 2007, Burns graduated from the Information Systems Officer course at the U.S. Army's School of Information Technology at Fort Gordon, Georgia.

**10810 Glenbarr DR**
**Johns Creek, GA 30097**
**Phone: 678- 548-9927**
**E-mail: Phillip.G.Burns.mil@mail.mil**

## REFERENCES

1. Frost and Sullivan, "The 2011 (ISC)2 Global Information Security Workforce Study." 13 May 2013 <https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf>
2. Wall, Andru. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." Harvard National Security Journal 3 (2011).
3. Ibid.
4. Lawrence, Susan. "Network Information Brief: Improving Network Security and Operational Effectiveness." 7 June 2012 <http://ciog6.army.mil/LinkClick.aspx?fileticket=04Ezkdq_fGU%3D&tabid=36>.
5. Ibid.
6. Mackert, Donald. "Cloud Computing Operational View 1 from the Data Center to the Tactical Edge." (email communication, 9 April 2013).
7. Mell, Peter, et. al. "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Science and Technology." September 2011 < http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
8. Burns, Phillip. "IT Governance: Key to Security." Military Information Technology 15.9 (2011): 21.
9. Ibid.
10. Lockhart, David. "Technology Brief: Protection for a Mobile Workforce." (email communication, 24 February 2013).
11. Ibid.
12. Multiple Authors. "A Primer on Electronic Document Security: How Document Control and Digital Signatures Protect Electronic Documents." 9 April 2013 <http://www.adobe.com/security/pdfs/acrobat_livecycle_security_wp.pdf >.