16th ICCRTS

“Collective C2 in Multinational Civil-Military Operations”

Cyber Security to the Edge: Applying Edge Theory to Cyber Security Operations

Topics

Topic 11: Cyberspace Management
Topic 2: Approaches and Organizations
Topic 5: Collaboration, Shared Awareness, and Decision Making

Name of Author
Chris Simpson
San Diego, CA

Point of Contact
Chris Simpson
Independent Researcher
Telephone: 619-865-7294
Email: csimpson4@mac.com

Abstract

Defending Department of Defense networks is a complex endeavor. Our current method of defending networks starts with topdown rules, policies and regulations. These rules and regulations are complex and in many cases may be redundant or contradicted to meet an urgent operational requirement. Additionally the requirements contained in these policies are not always funded. This paper will examine if edge organizational techniques and Edge Theory could be applied to cyber security organizations to improve the defense of DoD networks.

Introduction

Defending Department of Defense networks is a complex endeavor with an extensive amount of topdown rules, policies and regulations. These rules and regulations are complex and in many cases may be redundant or contradicted to meet an urgent operational requirement. In some cases new rules are created across the enterprise in response to a specific event at one part of the organization (i.e. Wiki leaks) without much thought to the impact on the entire organization. Additionally the requirements contained in these policies are not always funded. DoD networks could be better defended by organizing as an edge organization. This paper will introduce this concept and start the discussion to examine if edge organizational techniques and edge theory could be applied to cyber security organizations to improve the defense of DoD networks.

Edge Theory

In order to understand why an Edge organization will improve the performance of a cyber security organization we must have a common definition of an Edge organization and understand the characteristics of an Edge organization. Alberts defines an Edge organization as "Edge organizations are organizations where everyone is empowered by information and has the freedom to do what makes sense" [1]. Members in an Edge organization members are empowered to share information and most relationships are of a peer-to-peer nature. This eliminates the distinction between line and support personnel as well as the associated stovepipes of that artificial division. By flattening an organization the requirement for the "middle" part of an organization that relays communications within that organization is greatly reduced. This reduction of the "middle" and stovepipes removes "barriers to information sharing and collaboration" within that organization and between the components of that organization [1].

Current Top Down Structure

Under our current cyber structure senior leadership develops high level and detailed policy guidance along with extensive reporting requirements. The DoD Information Assurance Technology Analysis Center has a chart (Figure 1) that displays all of the guidance required to "Build and Operate a Trusted GIG" [2].

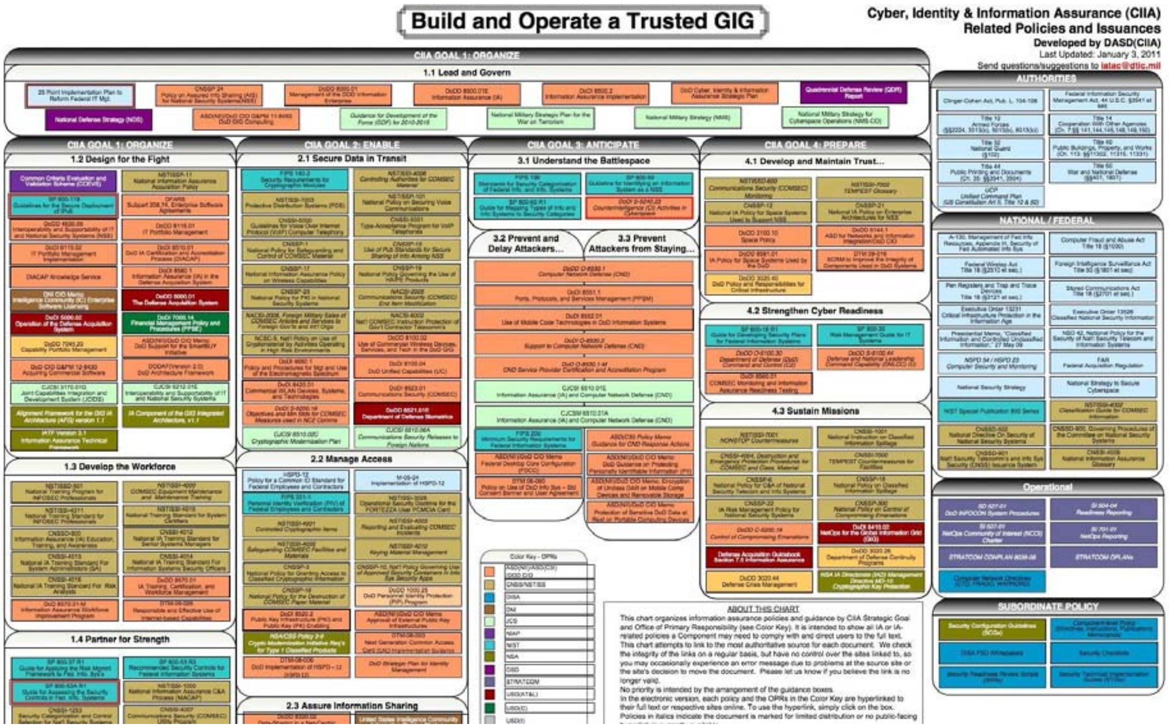
Build and Operate a Trusted GIG
Cyber, Identity & Information Assurance (CIIA)
Related Policies and Issuances
Developed by DASD(CIIA)
Last Updated: January 3, 2011
Send questions/suggestions to iatac@dtic.mil
CIIA GOAL 1: ORGANIZE
1.1 Lead and Govern
AUTHORITIES
CIIA GOAL 1: ORGANIZE
1.2 Design for the Fight
CIIA GOAL 2: ENABLE
2.1 Secure Data in Transit
CIIA GOAL 3: ANTICIPATE
3.1 Understand the Battlespace
CIIA GOAL 4: PREPARE
4.1 Develop and Maintain Trust...
3.2 Prevent and Delay Attackers...
3.3 Prevent Attackers from Staying...
4.2 Strengthen Cyber Readiness
4.3 Sustain Missions
NATIONAL / FEDERAL
1.3 Develop the Workforce
2.2 Manage Access
Operational
Color Key - OPRs
ABOUT THIS CHART
SUBORDINATE POLICY
1.4 Partner for Strength
2.3 Assure Information Sharing

Figure 1 (IATC 2011)

In addition to this high level and detailed DoD guidance there is an abundance of similar guidance at the service and operational level. In many cases the operational guidance is a copy of the high level guidance. Although the chart depicts the policy and divides them up into functional areas there is no mapping of policy relationships. For example the DoD Information Assurance Certification and Accreditation Process (DIACAP) policy does not map to the prevention and delaying attacks guidance so the people actually defending the networks and information systems may not have any visibility into the certification packages, which describe how systems are secured and associated risks, of the systems they are defending.

This centralized planning model does not lend itself to quick and agile defense of cyber assets. For successful centralized planning the central leadership must be able to “make sense of the situation, maintain this understanding in the face of a dynamic environment, predict the future, develop an appropriate response strategy, decompose the response into a coherent set of executable tasks, allocate resources, task subordinates, monitor execution, and make adjustments as required, all in a timely manner” [1].

With the complexity of even one information system that has thousands, if not millions lines of code and a multitude of possible configurations a centralized organization can’t possibly maintain control and understand the diverse configurations of these systems. The complexity of the systems and multitude of attack vectors (email, malicious websites, brute force, social engineering, phishing, malicious insiders) inhibit the effectiveness of a centralized planning model. With the large scale number of attacks on DoD networks “The Pentagon's top information-security official, Robert Lentz, said the Defense Department detected 360 million attempts to penetrate its networks last year, up from six million in 2006“ [3].

With such a high number of attacks how can a hierarchical and centralized organization manage the response to so many attempted attacks? “Cyberwarfare is like maneuver warfare, in that speed and agility matter most”[4]. By moving to an edge cyber security organization and allowing action at the edge make it easier to defend and respond to cyber attacks.

The Fog of War in Cyber Warfare

Information overload is one of the major factors for "fog of war” in cyber warfare. If every organization followed the current rules they would conduct recurring vulnerability scans and this data would be fed into different databases so the chain of command would have a list of 1000’s of vulnerabilities but does this enhance the overall security of the scanned systems if the owners don’t have the tools or manpower to resolve those vulnerabilities? With the amount and complexity of this data there is no way for a centralized organization make sense of this. This is analogous to telling Platoon commander to defend a street block but instead of letting him deploy his troops he would first have to scan the block for vulnerabilities on a checklist and submit those vulnerabilities to higher HQ. Many of the vulnerabilities on the checklist might not be applicable to the current situation, higher headquarters would asses the listed vulnerabilities them and tell the Platoon Commander which ones to fix. As this data makes its way up the chain of command the enemy disposition is constantly changing and by the time a response is received from upper echelon it may be too late to defend the block. Instead of doing this the Army develops tactics, techniques and procedures (TTPs) for the Platoon Commander to utilize that can be modified based on the local situation.

The attacker has the advantage in cyber warfare, the attacker only needs to know one vulnerability to gain access to a system while the defender must monitor all vulnerabilities. This advantage is increased when a defender operates in a hierarchical organization and must wait for top down direction to take action. Local units defending their own networks would have a smaller footprint and less data to monitor making it easier to detect attacks.

Cyber Warfare Command and Control

Even in an edge organization leadership must be involved in setting overall guidance and have situational awareness to the overall health of their systems. Under current vulnerability system the status individual systems are reported up the chain of command. A commander doesn’t need to know the exact status of each system, rather he needs to know the impact of those vulnerabilities. In an edge organization the commander would establish high level goals and requirements. A good example of establishing high level guidance is the “Ten Things Every Airman

Must Know in the United States Air Force Doctrine Document 3-12 of 15 July 2010 “Cyberspace Operations”:

1. The United States is vulnerable to cyberspace attacks by relentless adversaries attempt ing to infiltrate our networks at work and at home – millions of times a day, 24/7.
2. Our enemies plant malicious code, worms, botnets, and hooks in common websites, software, and hardware such as thumbdrives, printers, etc.
3. Once implanted, this code begins to distort, destroy, and manipulate information, or ―phone‖ it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.
4. The enemy attacks your computers at work and at home knowing you communicate with the Air Force network by email, or transfer information from one system to another.
5. As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates, and your country.
6. You significantly decrease our enemies’ access to our networks, critical USAF information, and even your personal identity by taking simple action.
7. Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.
8. Do not connect any hardware or download any software applications, music, or information onto our networks without approval
9. Encrypt sensitive but unclassified and/or critical information. Ask your computer systems administrator (CSA) for more information
10. Install the free Department of Defense anti-virus software on your home computer. Your CSA can provide you with your free copy” [5].

This guidance is easy too understand and implement. One can boil down the current policy to some similarly simply stated goals that could be implemented in an edge Organization:

1. Resilient network and information systemsBuild resilience at local level
2. Design secure systems from the start
3. Secure your system from current known vulnerabilities and monitor for attacks on open vulnerabilities
4. Monitor your system
5. Correlate attacks to known vulnerabilities
6. Respond to attacks
7. Communicate with higher headquarters

(Author’s interpretation of guidance listed on IATC 2011 [2])

Creating an Edge Cyber Security Organization

In order to become an edge cyber security organization we should consider locations as nodes on a network and empower those nodes to defend themselves and their neighbors. The term neighbors is used in the relationship between nodes on a network not their physical location. The first step would be to identify the policy that enhances cyber security, for example manning requirements to defend a local enclave. The next step can be done by providing pre built templates like the current Defense Information System Agency Gold Disk templates for common functions and let them develop defense for their unique systems. These nodes would also need visibility into their local network traffic and tools to asses their local vulnerabilities. There are already a variety of tools in use by the DOD that can accomplish this. They would also communicate with their neighbors and gain value by some type of mutual defense. To test the effectiveness of an edge organization a test enclave could be established that is empowered to defend their own network and communicate directly with anyone along their network path. Although a detailed test would have to be developed, below are some areas that could be measured to see the effectiveness of an edge organization [6]:

Quality of organic information

- Awareness of what is on the enclave

- Awareness of attacks (successful and unsuccessful

- Awareness of vulnerabilities

Quality of organic Information

Quality of Individual Sense making

- Do the operators understand what is on their network

Quality of interactions

Degree of shared information

Extent: Measure flow of information from enclave to neighboring enclaves, CND service providers, and higher HQ. This could be measured by: exchange of correlating IDS alerts, exchange of vulnerability alerts and status of connected systems (i.e. Vulnerabilities, accepted risk) [6].

The data collected from this test could be compared with similar data from other enclaves to see if there was an improvement in overall security

In many cases a cyber security event in one node can impact another node or have a broader impact to the organization. Systems that have any possibility of impacting outside of a node or that can have a broader impact on the enterprise would have to be identified and specific reporting requirements would have to be developed to notify the chain of command with appropriate time reporting requirements. This could be accomplished in many ways including the use of auto-reporting network sensors. Some examples of automatic external reporting requirements:

- Public exposure of sensitive or classified data

- Identification of self replicating worm
- Insider attack from one node to another

It is difficult for non security experts to understand the current way security incidents are handled. To better illustrate this the story below applies the methods we use to respond to computer attacks to the Navy Medical system.

Applying the Current Cyber Defense Workflow to the Medical System

Seaman Timmy (compromised computer) assigned to a ship catches the flu. The Navy Medical Command (Service Computer Emergency Response Team)in Bethesda, MD sends the corpsman on the ship an alert (intrusion detection alerts) that someone, but not a specific person, is sick and that he needs to be isolated immediately. The corpsman must search the ship to find the sick Sailor. Once found the corpsman must contact the medical command and receive guidance on how to aid Seaman Timmy. If the corpsman doesn't answer all questions there may be additional questions. The Medical Commands directive to isolate Seaman Timmy may endanger the ship since Seaman Timmy is the helmsman, steering the ship while at sea, (critical system). Once all of the information has been received by the medical command they will tell the corpsman to respond. Lets say the diagnose is a bacterial infection the medical command may prescribe an antibiotic. Since they don't have access to Seaman Timmy's medical record (DIACAP package) they may not know he is allergic to antibiotics putting him at risk.

How would an edge organization better handle the response to a computer attack? First a local sensor or other cueing detects compromised host. Local network defender locates system and determines criticality of the system. Since they know the most about the system they can take the best steps to immediately isolate that system with the least impact. The local defenders would also know the system's relationship and possible impact to connected systems and could alert adjacent system defenders as appropriate.

Conclusion

Defending the global information grid against attacks from Nation States, individual hackers, organized crime and malicious insiders is a complex task and problem. Solving complex problems requires innovative solutions that push down responsibility and empower people at the local level to defend their networks and systems. Self organized groups of defenders in an edge organization offers many advantages to the current top down hierarchal structure. These advantages include quicker response to network attacks by empowering individuals at the unit level, resilient networks by improving information sharing and reducing the administrative burden by removing redundant policy and flattening the cyber security organization. Higher echelons would have better situational awareness because they could focus on information from the edge that has been identified as critical rather that sifting through huge amounts of data reports without context.

References

[1] Alberts, D.S. and Hayes, R.E. (2003). *Power to the Edge*. Washington, DC: CCRP.

[2] Build and Operate a Trusted GIG. (2011). [Cyber, Identity &Information Assurance (CIIA) Related Policies and Issuances]. Information Assurance Technology Analysis Center. Retrieved from: http://iac.dtic.mil/iatac/download/ia_policychart.pdf

[3] Dreazen, Y.J. And Gorman, S. (6 May 2009). U.S. Cyber Infrastructure Vulnerable to Attacks.
Wall Street Journal. Retrieved from
http://online.wsj.com/article/SB124153427633287573.html

[4] Lynn, William. (2010). Defending a New Domain: the Pentagon's Cyberstrategy. U.S. Department of Defense. Retrieved from
http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx

[5] United States Air Force (USAF). (2010). *Cyberspace Operations* (Air Force Doctrine Document 3-12). Retrieved from ttp://www.airforce-magazine.com/SiteCollectionDocuments/The DocumentFile/Strategy%20and%20Concepts/AFDD3-12.pdf

[6] Office of Force Transformation. (2003). Network Centric Operations Conceptual Framework Version 1.0. Vienna, VA: Evidence Based Research.