AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Defending Critical Infrastructure as Cyber Key Terrain

by

Derek Molle, Civ, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Dr. Fred Stone

Maxwell Air Force Base, Alabama

August 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Table of Figures and Tables

Preface

Several years ago, under the personal belief that the weak cybersecurity of industrial control systems endangered national security, I began to seek out ways and means to better secure these vulnerable systems. In the subsequent years these reality of the danger began to become clear as news of real, large-scale destruction caused by malware including Stuxnet, Shamoon, Havex, and Blackenergy 2 all gathered international attention. While complete success is still far off, this study attempts to bring together some of what I have learned thus far. I extend my sincerest thanks and gratitude to my friends and colleagues in the 38th Cyberspace Engineering Group, Idaho National Laboratory, ICS-CERT, and the Information Assurance Directorate. I also have to thank my professor and classmates at the Air Command and Staff College as they helped guide me on my path to a successful completion of this arduous course. Without their assistance, this work would not have had the same impact or come to the same meaningful conclusions. Thank you!

Abstract

This study first examines the problems which necessitate cyber defense of critical infrastructure, then develops criteria necessary for successful cyber defense. Five alternative solutions are introduced as evolutions from two solutions by Kuipers and Fabro: Stand Alone Networks, Converged Enterprise Networks, Logically Isolated Enclaves, Logically Isolated Enterprises, and Stand Alone Enterprises. Based on their estimated ability to fulfil the criteria derived from Department of Defense doctrine, commercial best practice, and recommendations from the Department of Homeland Security and the National Security Agency, this study found that for short term mission assurance of specific cyber key terrain, creation and defense of a Logically Isolated Enclave can be accomplished immediately and with near zero cost by a Cyber Protection Team. Long term mission assurance still requires an enterprise solution for cyber defense of critical infrastructure. The pursuit of a Logically Isolated Enterprise is estimated to provide the best solution for cyber defense of critical infrastructure by extending and enhancing the existing capabilities in the corporate network operations and security center to the logically isolated control system enterprise.

.

I. Introduction

The cyberspace component of critical infrastructure presents an unmitigated vulnerability to the United States Air Force's warfighting capability.[1] The National Military Strategy for Cyberspace Operations, National Strategy to Secure Cyberspace, Quadrennial Defense Review and Department of Defense Cyber Security Strategy, show the problem is well known on a national level, however, steps must still be taken to address it. The 2006 National Military Strategy for Cyberspace Operations (NMS-CO) identifies strategic military superiority in cyberspace as the Department of Defense's strategic goal.[2] To achieve national level goals and objectives, all Combatant Commands, Military Departments, and other Defense Components require the ability to operate unhindered in cyberspace.[3] The NMS-CO is not specific to critical infrastructure but the United States' National Strategy to Secure Cyberspace (NSSC) is as it lists three strategic objectives:[4]

1) Prevent cyber attacks against America's critical infrastructures;

2) Reduce national vulnerability to cyber attacks; and

3) Minimize damage and recovery time from cyber attacks that do occur.

The primary concern behind these strategic objectives is of the threat of a cyber attack upon critical infrastructure capable of debilitating the national economy or national security capabilities. The NSSC acknowledges that no such attack has occurred today and responds that this is partially due to high technical sophistication of such an attack.[5]

The *2010 Quadrennial Defense Review* also noted the importance of operating effectively in the cyberspace domain, and outlined the steps the DoD is taking to strengthen its capabilities in this domain:[6]

- Develop a comprehensive approach to DoD operations in cyberspace

- Develop greater cyberspace expertise and awareness
- Centralize command of cyberspace operations
- Enhance partnerships with other agencies and governments

Then, as awareness of the cyber threat to critical infrastructure increased, the subsequent 2014 Quadrennial Defense Review noted "potential adversaries are actively probing critical infrastructure throughout the United States and in partner countries, which could inflict significant damage to the global economy and create or exacerbate instability in the security environment."[7] Furthermore, "The Department of Defense remains committed to working with industry and international partners as well, sharing threat information and capabilities to protect and defend U.S. critical infrastructure, including in our role as the sector-specific agency for the defense industrial base."[8] The Department of Defense Cyber Security Strategy summarizes the problem, "During a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage... Leaders must take steps to mitigate cyber risks." [9]

Research Focus

Defensive measures are essential to the mitigation of cyber risk. Therefore, an important question to ask is: In the context of critical infrastructure, what is the best way to defend cyber key terrain?

This research applies a problem-solution framework to the study of defending critical infrastructure as cyber key terrain. While not performing an evaluation against a single Air Force system, this research studies cyber key terrain with consideration for unique aspects of critical infrastructure to explain the best way to defend critical infrastructure supporting warfighting capability for the DOD and critical business processes for businesses.

Overview

This study first develops the problems which necessitate cyber defense of critical infrastructure, then develops criteria necessary for successful cyber defense according to doctrine, commercial practice, and government recommended practice. Five alternative solutions are introduced based on varying levels of network isolation and duplication of network infrastructure then analyzed according to their estimated ability to fulfil the criteria developed. Recommendations and conclusions follow at the end of the study.

II. Description of Problem

Critical Infrastructure, cyber key terrain, Mission Assurance, and Shadow IT

The term critical infrastructure describes a variety of systems across numerous sectors. Critical infrastructure has been identified and organized into 16 sectors. The following sector specific agencies are responsible for their respective sectors of critical infrastructure: [10]

- Department of Agriculture – agriculture and food sector (meat, poultry, egg products);
- Health and Human Services -- public health and healthcare sector and the food sector (other than meat, poultry, egg products);
- Environmental Protection Agency -- drinking water and water treatment systems sector;
- Department of Energy – energy sector (including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities);
- Department of the Treasury -- banking and finance sector;
- Department of Defense -- defense industrial base sector.

The remaining 10 sectors of critical infrastructure were assigned to the Department of Homeland Security including: commercial facilities sector, chemical sector, communications sector, critical manufacturing sector, dams sector, emergency services sector, government facilities sector, information technology sector, commercial nuclear power facilities, materials, and waste sector, and transportation systems sector. [11] Since the information technology sector and communications sector are widely discussed in other studies, this study emphasizes cyberspace defense of critical infrastructure as a form of operational technology outside the bounds of standard information technology.[12]

As the name implies, cyber key terrain is key terrain in the cyberspace domain. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, does not directly define cyber key terrain, but it does define key terrain. Key terrain is defined as, "Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant."[13] Applying this definition of key terrain to cyberspace, a definition is derived which includes the interdependent network of computer systems, embedded processors, and controllers seizure or retention of which would afford an adversary an advantage which would in turn deny or degrade friendly forces from mission accomplishment. Furthermore, key terrain involves elements that enable mission essential warfighting functions, be they in a physical domain or in cyberspace, and those elements are temporal because they change with the mission and adversary.[14] The protection of key terrain is critical to mission assurance because it requires "actions taken to achieve mission resiliency and ensure the continuation of [Mission Essential Functions]."[15]

Mission assurance is the "actions taken to achieve mission resiliency and ensure the continuation of [Mission Essential Functions] and assets, including personnel, equipment, facilities, networks, information, infrastructure, and supply chains, so that the [Defense Intelligence Enterprise] can conduct its critical missions under all conditions and across the spectrum of threats and hazards."[16] To be successful in mission assurance, the mission must be assured on all levels, including physical and cyber. There is interdependency between critical infrastructure and mission essential warfighting functions.[17] Critical infrastructure connects the cyber domain to physical systems which, directly or indirectly, are essential to key business processes. Critical infrastructure is vulnerable to cyber-attack.[18] System owners are responsible for the operation of their systems while Combatant Commanders are responsible for “prevention of the loss or degradation” of critical infrastructure supporting Mission Essential Functions inside of their area of operations.[19] Existing practices tend to focus on information technology solutions and may not be adequate to defend cyberspace associated with critical infrastructure.

Network operations and security operations are the means by which information technology policy is applied to accomplish cyber defense. Network operations and security operations traditionally have little interaction with the installation level process engineers responsible for design, installation, operation, and maintenance of ICS. In turn, process engineers and operators are generally concerned with the continuous operation of the critical infrastructure more so than the cybersecurity posture of that same critical infrastructure. Isolation of security operators and process engineers results in Shadow Information Technology (IT).[20] Shadow IT describes information systems used inside of organizations without the approval of those organizations. Shadow IT is used in conjunction with the term Stealth IT which describes information systems specified and deployed by departments other than the IT department. Shadow IT typically violates implicit and explicit IT usage restrictions with the intention of enhancing or enabling work performance.[21] The mission cannot be assured in an environment where Shadow IT and Stealth IT are allowed to thrive because the cyberspace for those systems is left undefended.

Critical Infrastructure Interdependence and Mission Dependence

RAND Corporation’s Science and Technology Policy Institute found: "One of the most frequently identified shortfalls in knowledge related to enhancing critical infrastructure protection capabilities is the incomplete understanding of interdependencies between infrastructures."[22] Interdependency between infrastructures extends the attack surface of critical infrastructure to the infrastructure upon which it is dependent. For example, absolute cybersecurity of a power plant will be ineffective if a cyber attack upon transportation infrastructure prevents refueling.

In a 2006 survey of existing research for critical infrastructure interdependency modeling, Idaho National Laboratories showed how the energy sector, water sector, transportation sector, communications sector and emergency services sector all rely upon one another to function. No sector of critical infrastructure is fully independent yet most sectors are organized under separate functional leadership. As such, no single organization has the responsibility to assure operation for the infrastructure any given sector relies upon to function. The methodology Idaho National Laboratories used to study critical infrastructure interdependency was derived from concepts in effects-based operations and operations research called Operational Network Analysis.[23]

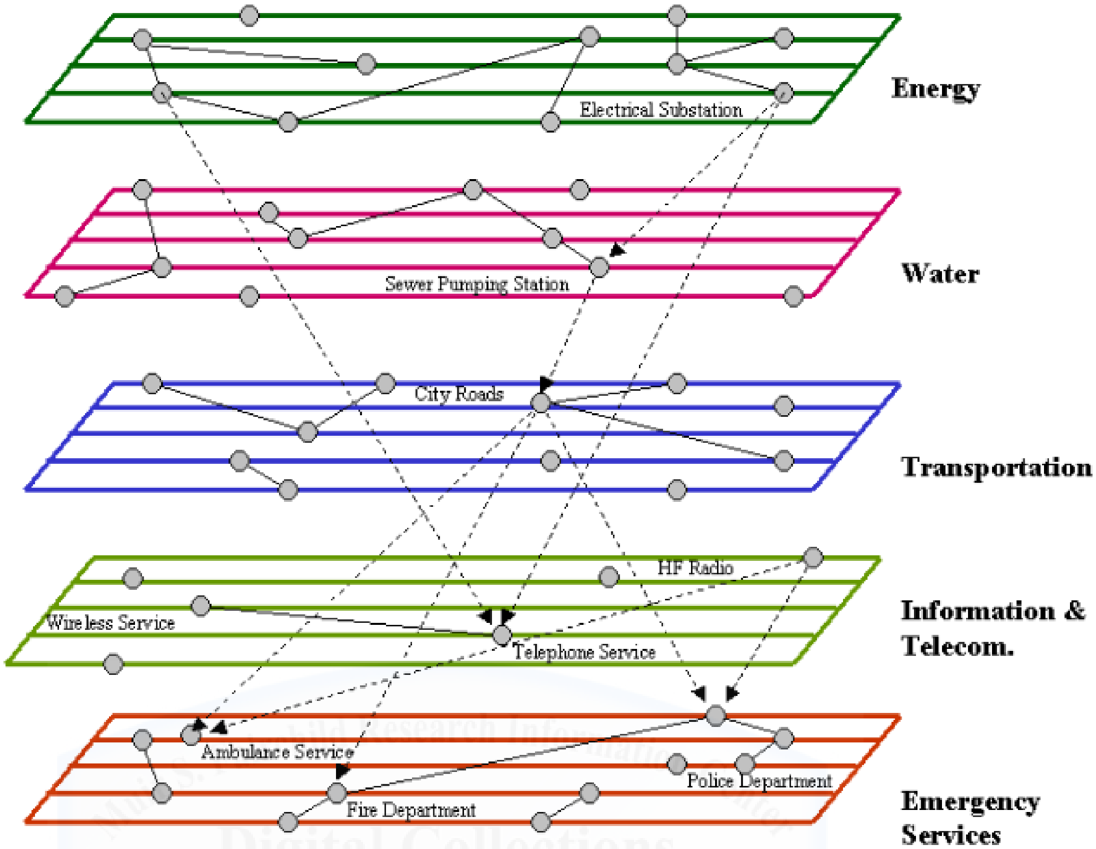


Figure 1: Interdependence of Critical Infrastructure (Reprinted from Peter Pederson, D. Dudenhoeffer, Steven Hartley, and May Permann, "Critical infrastructure interdependency modeling: a survey of US and international research." [Idaho National Laboratory, 2006]: 3.)

The interdependent nature of critical infrastructure makes the defense of each component necessary to the defense of the whole. The cyberspace domain intersects not only the information & telecommunications sector but each component of each sector as they are comprised of operational technology such as embedded systems or electronic controllers.

Because cyber key terrain depends upon the specifics of the mission that cyberspace is required for, the ability to operate through a cyber-attack upon critical infrastructure also depends on the specifics of the mission. Trepagnier and Schulz, however, found that in order to prevent failure of mission essential functions over large-scales of time or across large and interdependent networks, large scale mission assurance concepts require an enterprise defense of the entire network. [24] While Trepagnier and Schulz focused on mission assurance of information systems in general and not specifically operational technology associated with critical infrastructure, there are some similarities and differences.

The life span of information technology systems and operational technology systems differ by orders of magnitude. An information technology system might have a life span of six years while the life span of operational technology systems used by critical infrastructure often exceeds twenty years. [25] In order to replace the operational technology system, the infrastructure will often require simultaneous modernization together with the operational technology systems as new systems are no longer interoperable with twenty or thirty year old technology. Trepagnier and Schulz did not comment on the implications of life span beyond the “years” threshold but, it poses several challenges:

- Persistent malware can be considered more valuable on critical infrastructure because the infection is likely to last longer
- Older systems have more known vulnerabilities and exploits
- Host level mitigation of known vulnerabilities and exploits may require replacement of the operational technology system, which may not be possible without an expensive and simultaneous modernization of infrastructure

These challenges make critical infrastructure a desirable target not just for kinetic effect but also as the cyberspace equivalent to a beachhead for access to an organization’s internal network. To overcome these challenges, a long term enterprise defense focus that includes critical infrastructure is necessary to prevent the establishment of a cyber beachhead with access to the organization's internal network.

The concept behind Trepagnier and Schulz's work assumes each information system or host serves some purpose, that eventually each host will be called upon for that purpose, and that these systems exist upon a network. The purpose of a host might be obvious, such as the networked host used to control air traffic. The purpose of a host might also be obscure, such as monitoring of temperature in a room. Even hosts with an obscure purpose are sometimes essential because of network interdependency. The host used to monitor the temperature in a room might share that information with the building heating system to prevent water pipes from freezing and bursting. That water line might have been essential to fire protection systems, not to mention necessary for maintaining sanitary conditions in the building. [26] Not all critical infrastructure serves an obvious mission purpose; however, since research by Idaho National Laboratories shows interdependency among critical infrastructure sectors form a large and interdependent network, the Trepagnier and Schulz findings can be extended to critical infrastructure. Therefore, while warfighting capability may survive failures of critical infrastructure, the ability to sustain the fight collapses together with the failure of critical infrastructure as an Nth order effect because of system interdependency. [27]

The Geographic Combatant Commanders are Responsible but Not Equipped

The current paradigm of critical infrastructure protection, exemplified by Joint Publication 3-12: *Cyberspace Operations*, posits that "Defense critical infrastructure (DCI) refers to DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide that are a subset of Critical Infrastructure (CI) & Key Resources (KR). Geographic Combatant Commands (GCC) have the responsibility to prevent the loss or degradation of the DCI within their Areas of Responsibility (AOR) and must coordinate with the DOD asset owner, heads of DOD components, and defense infrastructure sector lead agents to fulfill this responsibility."[28] The defense of critical infrastructure is a problem faced by the Air Force and combatant commands are responsible for their defense.

In a joint letter published February 2016 to the United States Secretary of Defense, Admiral William Gortney, Commander of U.S. Northern Command, and Admiral Harry Harris, Commander of U.S. Pacific Command, described the lack of cybersecurity for Department of Defense critical infrastructure Industrial Control Systems (ICS) as an emerging threat with serious consequences to their ability to operate.[29] Both U.S. Northern Command and U.S. Pacific Command raise the issue of ownership of policies related to critical infrastructure, saying ownership is not clear across all levels of the Department of Defense, and the issue of equipment, saying tools and processes still require development.

III. Measurement Criteria

In this section, necessary and desirable capabilities are derived from three sources: doctrine, commercial practice, and government recommended practice. The ability of a cyber defense solution to possess these traits must be considered in the context of mission assurance.

Cyberspace Defense

Joint doctrine organizes internal defense of cyberspace into four components: Organic Defenses, Dedicated Defenses, Enterprise Defenders, and Cyberspace Protection Teams. [30]

Organic defense includes regular system administration such as system level monitoring, emergency patching, and reconfiguration to mitigate against system specific vulnerabilities. [31] In the case of critical infrastructure the process engineers, program management office, or functional system administrator performs this role. Dedicated defense describes cyberspace infrastructure that serves a purely defensive purpose such as intrusion detection and prevention systems, firewalls, antivirus, application whitelisting, and other boundary defenses. [32] Because critical infrastructure is a common kind of Stealth IT, it is often designed and installed without dedicated defenses[33]. Enterprise defenders are the personnel assigned to operate defensive cyberspace infrastructure and perform network defense activities. The enterprise defenders can also be referred to as the Computer Network Defense Service Providers or Cybersecurity Service Providers. DODI 8530.01 further details expected network defense activities as follows: [34]

- Vulnerability Assessment and Analysis
- Vulnerability Management
- Malware Protection

- Continuous Monitoring
- Cyber Incident Handling
- User Activity Monitoring for the DoD Insider Threat Program
- Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.

Cyberspace Protection Teams are deployable teams of cyberspace defense units specialized in identifying mission essential functions, cyber key terrain, and providing mission assurance as a secondary defense against advanced threats on a temporary basis. [35]

The Ten Strategies of a World-Class Cybersecurity Operations Center studies commercial best practices for the enterprise focal point for computer network defense, the security operations center:[36]

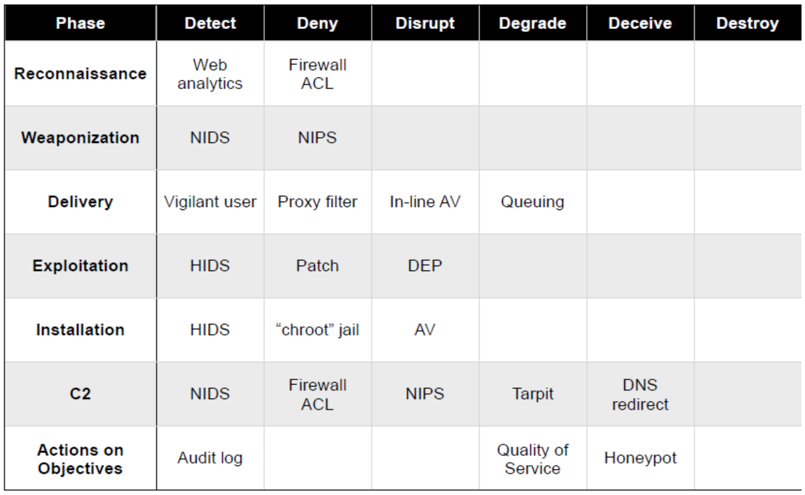
- Real-time Monitoring and Triage
- Incident Analysis, Coordination, and Response
- Cyber Intel Collection and Analysis
- Sensor Tuning and Management of the Security Operations Center Infrastructure's Operations and Maintenance
- Tool Engineering and Deployment

The security operations center is a commercial implementation of the enterprise defenders role. Nine key attributes are identified in the study: Programmatic, Instrumentation, Analytics and Detection, Monitoring, Threat Assessment, Escalation Response and Reporting, Situational Awareness, Prevention, Training and Career. [37] Programmatic attributes refer to the organization and authorities of the security operations center. A security operations center is most effective when it is a part of the organizations they serve and have written policy granting an authority to exist, procure resources, and enact change. A security operations center that is external to the organization it serves is generally less effective because of its limited ability to enact change.

Threat Evaluation and Mitigation Matrices

The study of threat evaluation and mitigation matrices as an analytical tool for the evaluation of cyber defense has been evolutionary. One of the earliest threat evaluation models was the Spoofing, Tampering, Repudiation, Information leak, Denial of Service, Elevation of Privilege (STRIDE) model popularized by Microsoft in 2007.[38] As an architecture-centric threat model, STRIDE attempts to identify what types of attack system elements may be vulnerable to. Once identified, organic and dedicated defenses can be employed to protect against exploitation of the vulnerability.

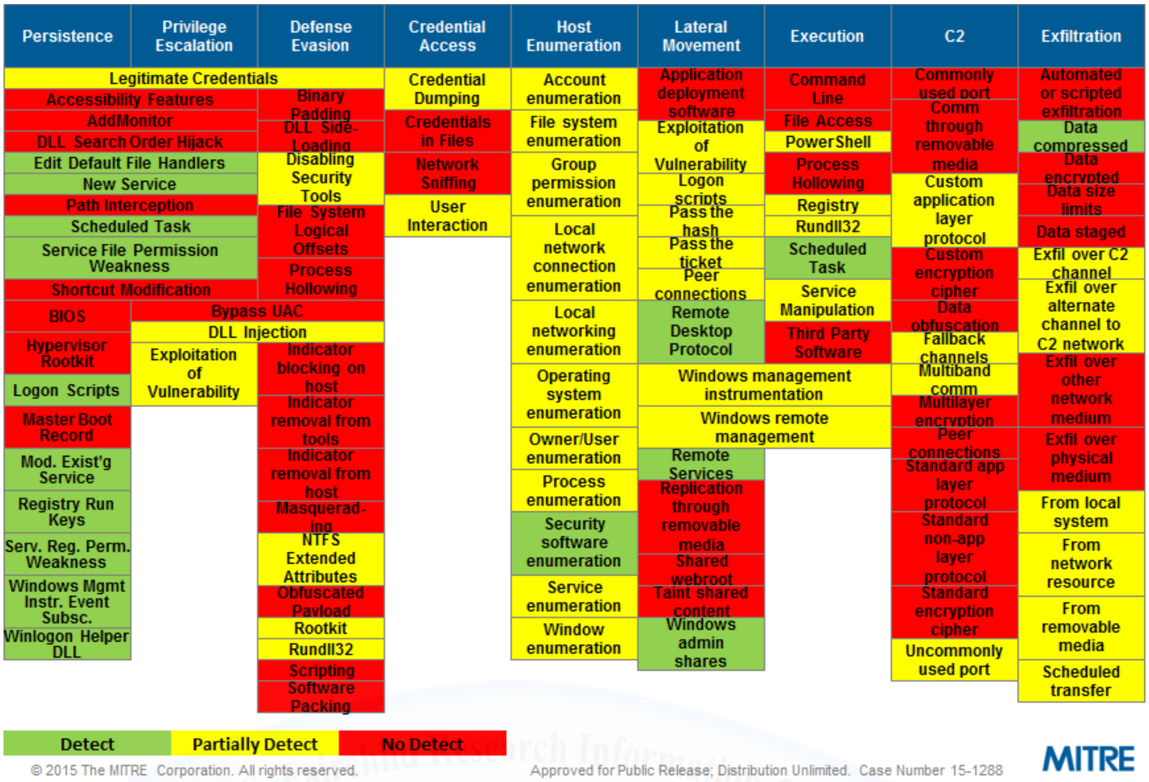
Hutchins is credited with the first phase based modeling approach to threat evaluation driven cyber defense.[39] The Intrusion Kill Chain phase model, later renamed the Cyber Kill Chain, is an attacker-centric threat evaluation model which describes seven phases of computer network exploitation and maps those phases against standard cyberspace targeting effects borrowed from what was at the time information operations doctrine.[40] The matrix, as shown in figure 3, is formed between Cyber Kill Chain phasing and countermeasure effects is used to identify what countermeasures can or should be used.



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Figure 2: Lockheed Martin Cyber Kill Chain Countermeasure Matrix (Reprinted from Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research Volume 1*, [Academic Conferences Limited, 2011]: 5.)

The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Model combines the architecture-centric approach used by the STRIDE model with the attacker-centric model used by the previous Cyber Kill Chain model.[41] The result focuses on creating a matrix which compares attacker objectives with tactics and system vulnerabilities, then describes how effective current countermeasures are expected to be.



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
🟨 Legitimate Credentials	🟨 Legitimate Credentials	🟨 Legitimate Credentials	🟨 Credential Dumping	🟨 Account enumeration	🟥 Application deployment software	🟥 Command Line	🟥 Commonly used port	🟥 Automated or scripted exfiltration
🟥 Accessibility Features	🟥 Accessibility Features	🟥 Binary Padding	🟥 Credentials in Files	🟨 File system enumeration	🟨 Exploitation of Vulnerability	🟥 File Access	🟥 Comm through removable media	🟩 Data compressed
🟥 AddMonitor	🟥 AddMonitor	🟥 DLL Side-Loading	🟥 Network Sniffing	🟨 Group permission enumeration	🟨 Logon scripts	🟨 PowerShell	🟨 Custom application layer protocol	🟥 Data encrypted
🟥 DLL Search Order Hijack	🟥 DLL Search Order Hijack	🟨 Disabling Security Tools	🟨 User Interaction	🟨 Local network connection enumeration	🟨 Pass the hash	🟥 Process Hollowing	🟥 Custom encryption cipher	🟥 Data size limits
🟩 Edit Default File Handlers	🟩 Edit Default File Handlers	🟥 File System Logical Offsets		🟨 Local networking enumeration	🟨 Pass the ticket	🟨 Registry	🟥 Data obfuscation	🟥 Data staged
🟩 New Service	🟩 New Service	🟥 Process Hollowing		🟨 Operating system enumeration	🟨 Peer connections	🟨 Rundll32	🟨 Fallback channels	🟨 Exfil over C2 channel
🟥 Path Interception	🟥 Path Interception	🟥 Bypass UAC		🟨 Owner/User enumeration	🟩 Remote Desktop Protocol	🟩 Scheduled Task	🟨 Multiband comm	🟨 Exfil over alternate channel to C2 network
🟩 Scheduled Task	🟩 Scheduled Task	🟨 DLL Injection		🟨 Process enumeration	🟨 Windows management instrumentation	🟨 Service Manipulation	🟥 Multilayer encryption	🟥 Exfil over other network medium
🟩 Service File Permission Weakness	🟩 Service File Permission Weakness	🟥 Indicator blocking on host		🟩 Security software enumeration	🟨 Windows remote management	🟥 Third Party Software	🟥 Peer connections	🟥 Exfil over physical medium
🟥 Shortcut Modification	🟥 Shortcut Modification	🟥 Indicator removal from tools		🟨 Service enumeration	🟩 Remote Services	🟨 Windows management instrumentation	🟥 Standard app layer protocol	🟨 From local system
🟥 BIOS	🟥 Bypass UAC	🟥 Indicator removal from host		🟨 Window enumeration	🟥 Replication through removable media	🟨 Windows remote management	🟥 Standard non-app layer protocol	🟨 From network resource
🟥 Hypervisor Rootkit	🟨 DLL Injection	🟥 Masquerading			🟥 Shared webroot		🟥 Standard encryption cipher	🟨 From removable media
🟩 Logon Scripts	🟨 Exploitation of Vulnerability	🟨 NTFS Extended Attributes			🟥 Taint shared content		🟨 Uncommonly used port	🟨 Scheduled transfer
🟥 Master Boot Record		🟥 Obfuscated Payload			🟩 Windows admin shares			
🟩 Mod. Exist'g Service		🟨 Rootkit						
🟩 Registry Run Keys		🟨 Rundll32						
🟩 Serv. Reg. Perm. Weakness		🟥 Scripting						
🟩 Windows Mgmt Instr. Event Subsc.		🟥 Software Packing						
🟩 Winlogon Helper DLL								

🟩 Detect 🟨 Partially Detect 🟥 No Detect

© 2015 The MITRE Corporation. All rights reserved.

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

Figure 3: Defensive Gap Analysis using the ATT&CK Matrix (Reprinted from The MITRE Corporation, "ATT&CK," [The MITRE Corporation, 20 May 2015]: https://attack.mitre.org/wiki/ATT%26CK_Matrix.)

The ATT&CK model has one serious deficiency in that all techniques are Microsoft Windows specific. While some critical infrastructure does operate on Microsoft Windows, most does not. Therefore, the ATT&CK model is more proof of concept than solution and requires tailoring prior to use in critical infrastructure environments. Threat evaluation and mitigation matrices do, however, provide a method for decomposition of cyber defense solutions and may be used to better understand how cyber defense measures protect against cyberattack.

Defense-in-Depth

The Industrial Control System Computer Emergency Response Team highlights five high level goals and seven detailed cyberspace defense strategies to defend critical infrastructure:[42]

- Cyberspace Defense Goals
    - Create and Enforce Security Policies
    - Blocking Unauthorized Access to Resources and Services
    - Detecting Malicious Activity
    - Mitigating Possible Attacks
    - Fixing Core Problems
- Cyberspace Defense Strategies
    - Implement Application Whitelisting
    - Ensure Proper Configuration/Patch Management
    - Minimize the Attack Surface
    - Build a Defensible Environment
    - Manage Authentication
    - Monitor and Respond
    - Implement Secure Remote Access

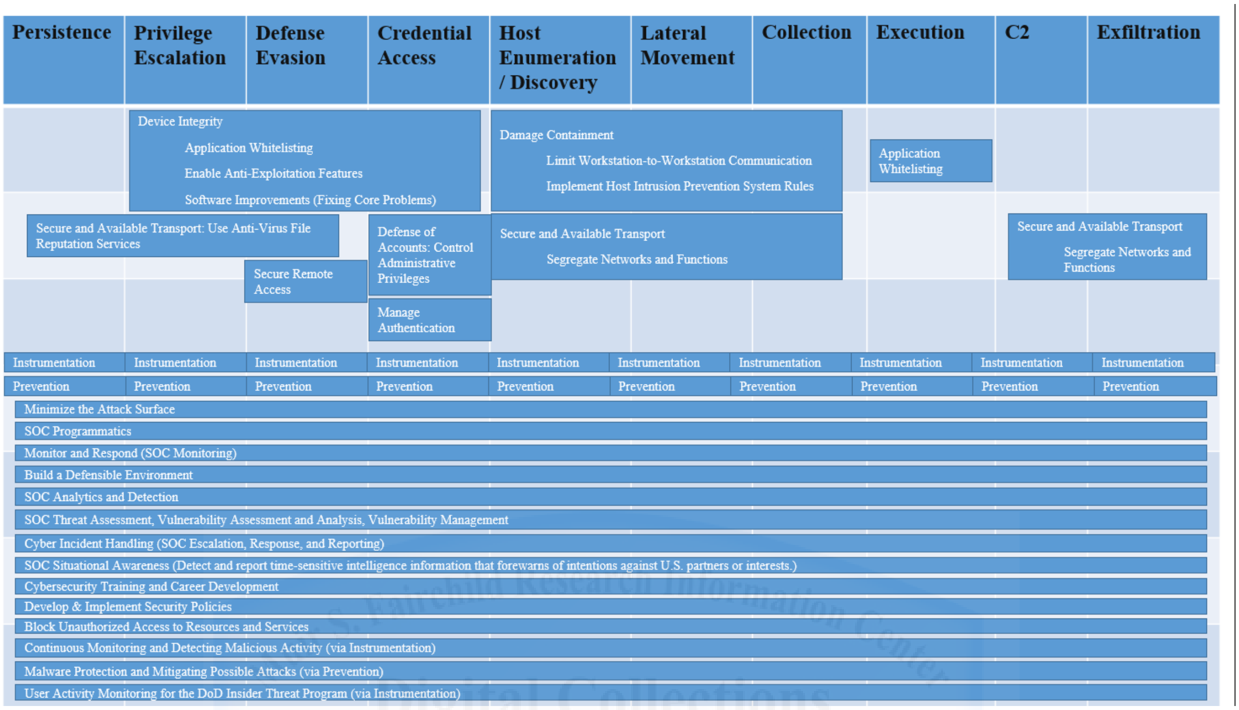
The National Security Agency's Information Assurance Directorate identifies four mitigation goal areas and ten technical mitigations which they believe should be pursued to create a layered defense with the ability to "fight through" cyber-attack:[43]

- Device Integrity
    - Application Whitelisting

  - Enable Anti-Exploitation Features
  - Set a Secure Baseline Configuration
  - Take Advantage of Software Improvements
- Damage Containment
  - Limit Workstation-to-Workstation Communication
  - Implement Host Intrusion Prevention System Rules
- Defense of Accounts
  - Control Administrative Privileges
- Secure and Available Transport
  - Use Anti-Virus File Reputation Services
  - Use Web Domain Name System (DNS) Reputation Services
  - Segregate Networks and Functions

The Industrial Control System Computer Emergency Response Team and Information Assurance Directory recommend these overarching defensive measures and cyber defense solutions are measured against their inclusion of these measures. However, since critical infrastructure networks should not rely on external DNS, the recommendation for web domain name system reputation services can be excluded.

Consequently, the best cyberspace defense solution is dependent on both the capability of the attacker, the control system network architecture, and vulnerability of the critical infrastructure itself. Overarching defensive measures exist that will be used as the criteria of this study, as represented in the cyber kill chain aligned mitigation matrix below:



Persistence | Privilege Escalation | Defense Evasion | Credential Access | Host Enumeration / Discovery | Lateral Movement | Collection | Execution | C2 | Exfiltration

Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)

Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules

Application Whitelisting

Secure and Available Transport: Use Anti-Virus File Reputation Services

Secure Remote Access

Defense of Accounts: Control Administrative Privileges

Manage Authentication

Secure and Available Transport
Segregate Networks and Functions

Secure and Available Transport
Segregate Networks and Functions

Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation | Instrumentation

Prevention | Prevention | Prevention | Prevention | Prevention | Prevention | Prevention | Prevention | Prevention | Prevention

Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 4: Critical Infrastructure Cyber Kill Chain Aligned Mitigation Matrix

IV. Alternative Descriptions

Stand Alone Network

The traditional solution to cyber defense of critical infrastructure has been isolation as illustrated by Kuipers and Fabro.[44] In this alternative, connectivity exists between the corporate network and the critical infrastructure control system network. Due to operational requirements for remote access, external VPN access is established through a router connected to the control system network and to several servers but not connected to the corporate network. Also due to operational requirements for communication between the control system network and remote field locations, a dial-up modem pool is combined with wireless access points to connect field locations directly into the data acquisition server because the control system local area network could not be physically extended to those locations. Common IT services such as email and web access are typically not available inside of the control system network because of isolation from the internet and the corporate network. This isolation also limits or prevents network and security operations teams from accessing the control system network.

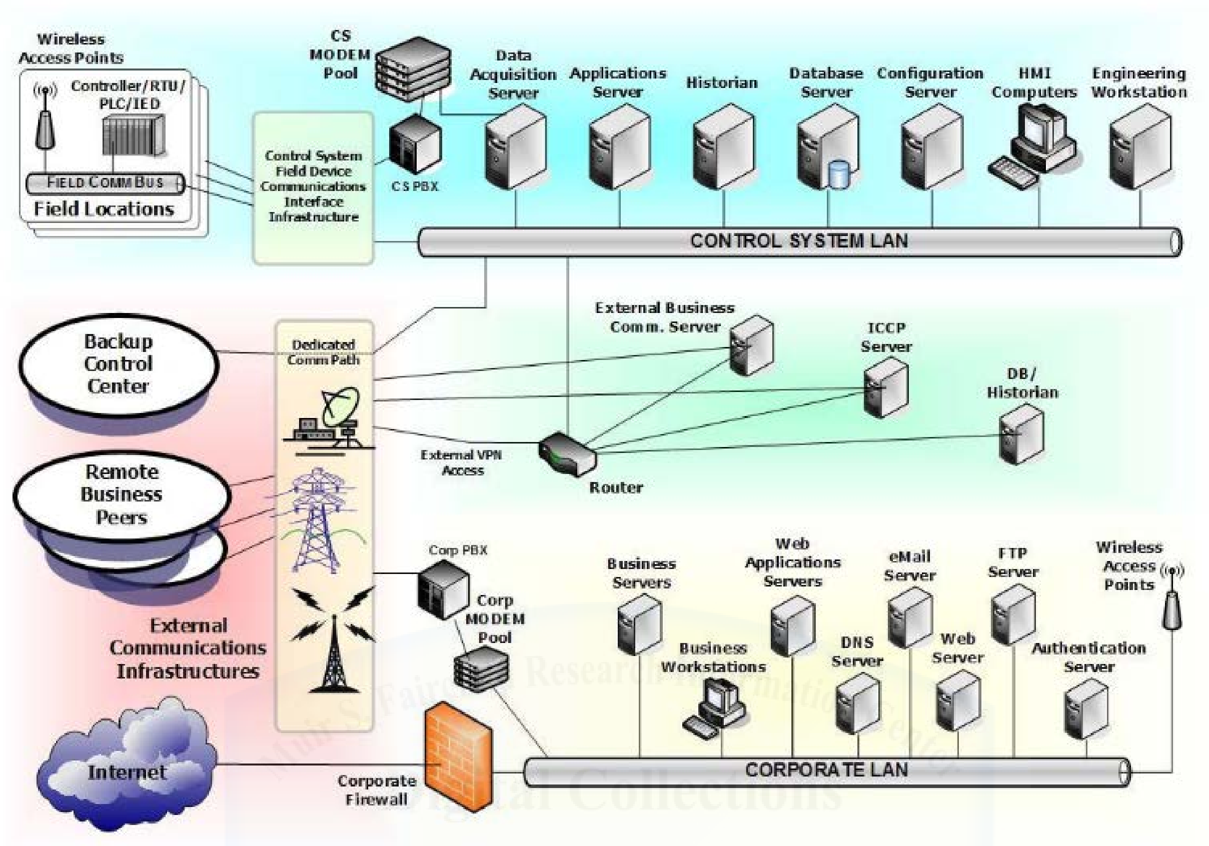


Figure 5: Stand Alone Network Architecture (Reprinted from David Kuipers and Mark Fabro. "Control Systems Cyber Security: Defense in Depth Strategies," [United States: Department of Energy, 2006]: 4.)

Converged Enterprise Network

Following a larger trend towards network convergence, the converged network approach leverages IP convergence and integrates the corporate network and the control system network into one network.[45] Due to operational requirements for remote access, external VPN access is established through a router connected to the converged network and to several servers. Leveraging the ubiquity of the corporate IP network, a dial-up modem pool is not required to connect field locations directly into the converged corporate/control system network. The network operations and security operations teams have as much access and visibility into the control system network as it does the corporate network. In large networks, it is possible for the network operations and security operations teams to be unable to differentiate between information technology assets and operational technology assets. Depending on network policy, web access and email access may be available to process engineers on a shared Engineering/Corporate workstation. This lack of differentiation can sometimes result in self-inflicted denial of service after untested patches or vulnerability scans are applied to operational technology.[46]

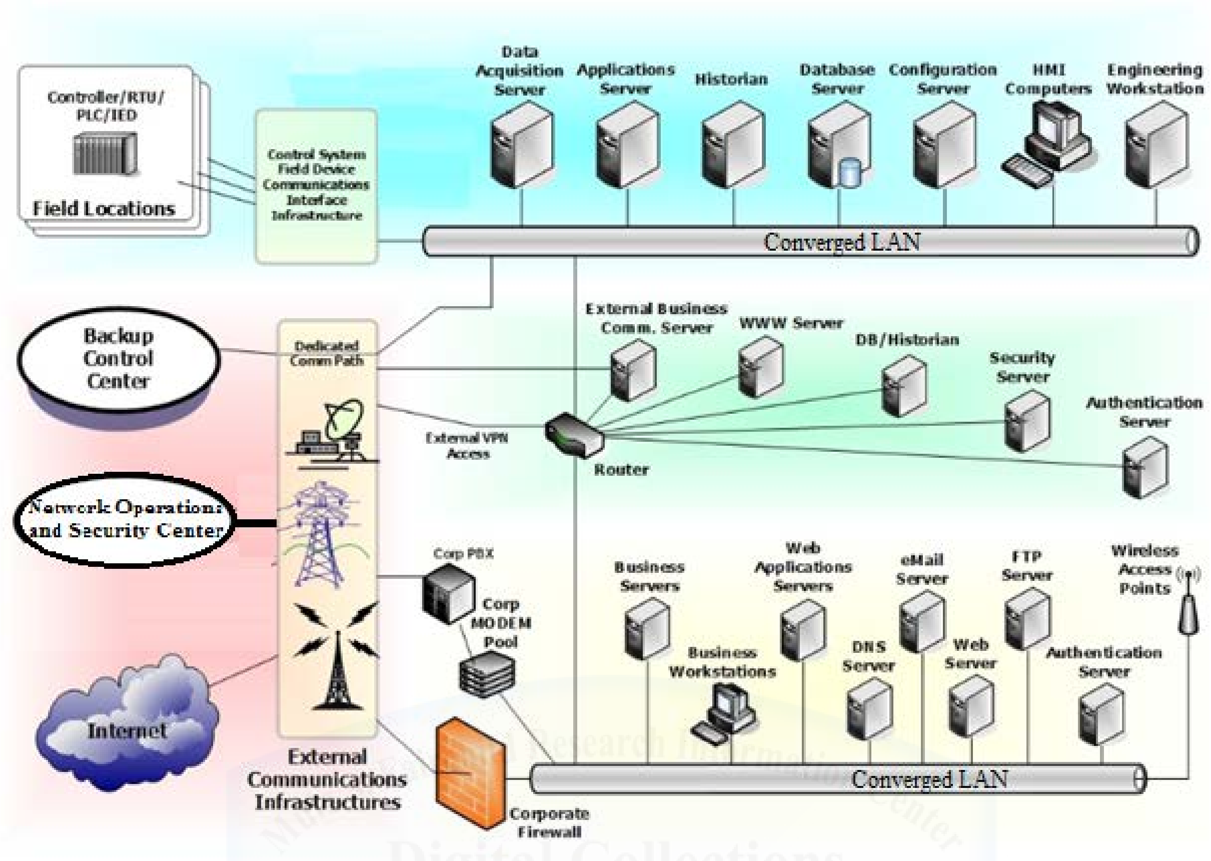


Figure 6: Converged Enterprise Network Architecture (Adapted from David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” [United States: Department of Energy, 2006]: 6.)

Logically Isolated Enclave

The logically isolated enclave approach leverages the advantages of network convergence by enabling the extension of the control system network enclave over existing IP-enabled corporate network infrastructure while also isolating the control system network into a logically separated network using virtualized routers and virtualized local area network. Traffic is not permitted into the enclave to maintain isolation; however, some traffic is permitted outbound such as SMTP alerts and antivirus detection alerts.[47] The isolation provided by this topology can be considered equivalent to the isolation provided by a physically separate network except in the event that the corporate network infrastructure itself is compromised and becomes malicious. The Network Operations and Security Center in this alternative receives information from the Control System network

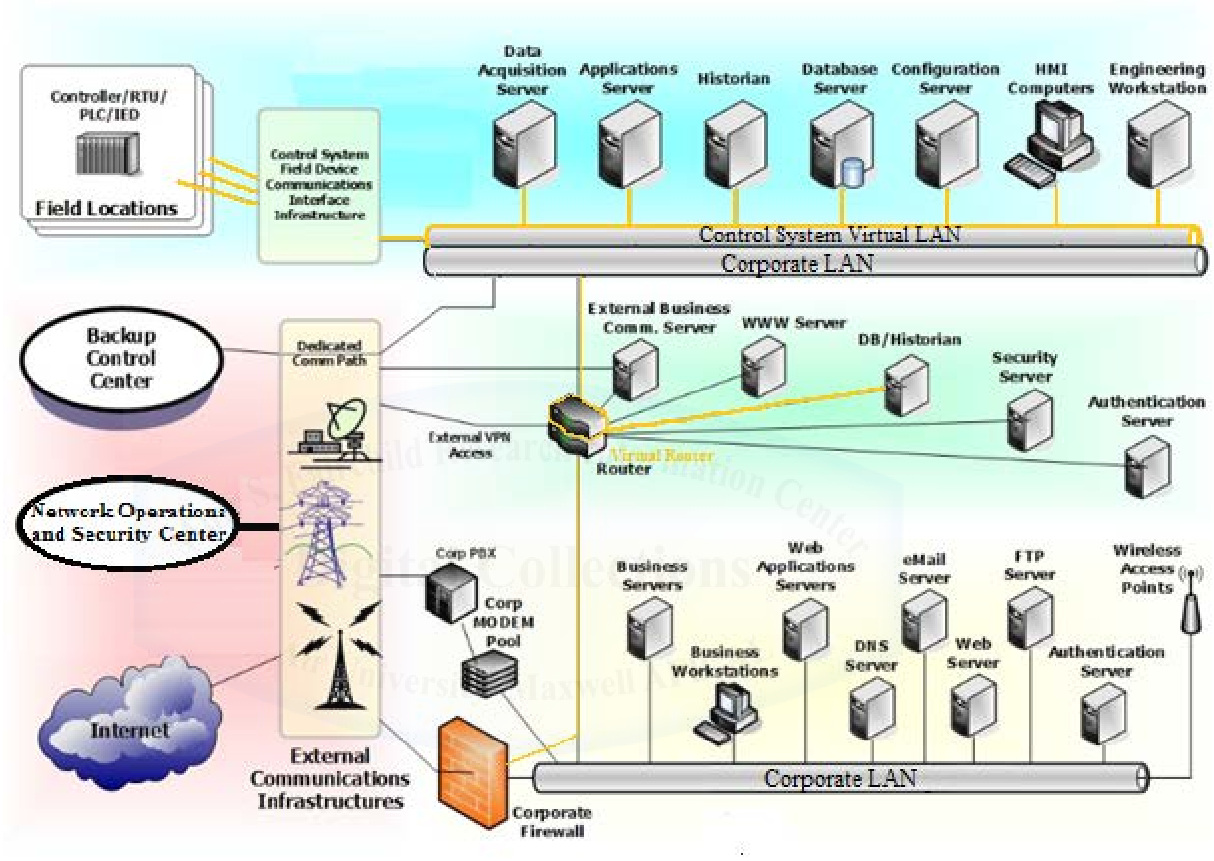


Figure 7: Logically Isolated Enclave Architecture (Adapted from David Kuipers and Mark Fabro. "Control Systems Cyber Security: Defense in Depth Strategies," [United States: Department of Energy, 2006]: 6.)

Logically Isolated Enterprise

The logically isolated enterprise extends and interconnects multiple logically isolated enclaves through a security appliance, i.e. the corporate firewall, and provides direct access to a common enterprise network operations and security operations team with separate organic and dedicated defenses. The enclave level firewall enables the network operations and security operations team to segment the enterprise network and limit lateral movement across the control system enterprise. Unlike the fully converged network approach, this cyber defense alternative requires duplication of equipment at the network operations and security center to support both a corporate network as well as the control system network.

.

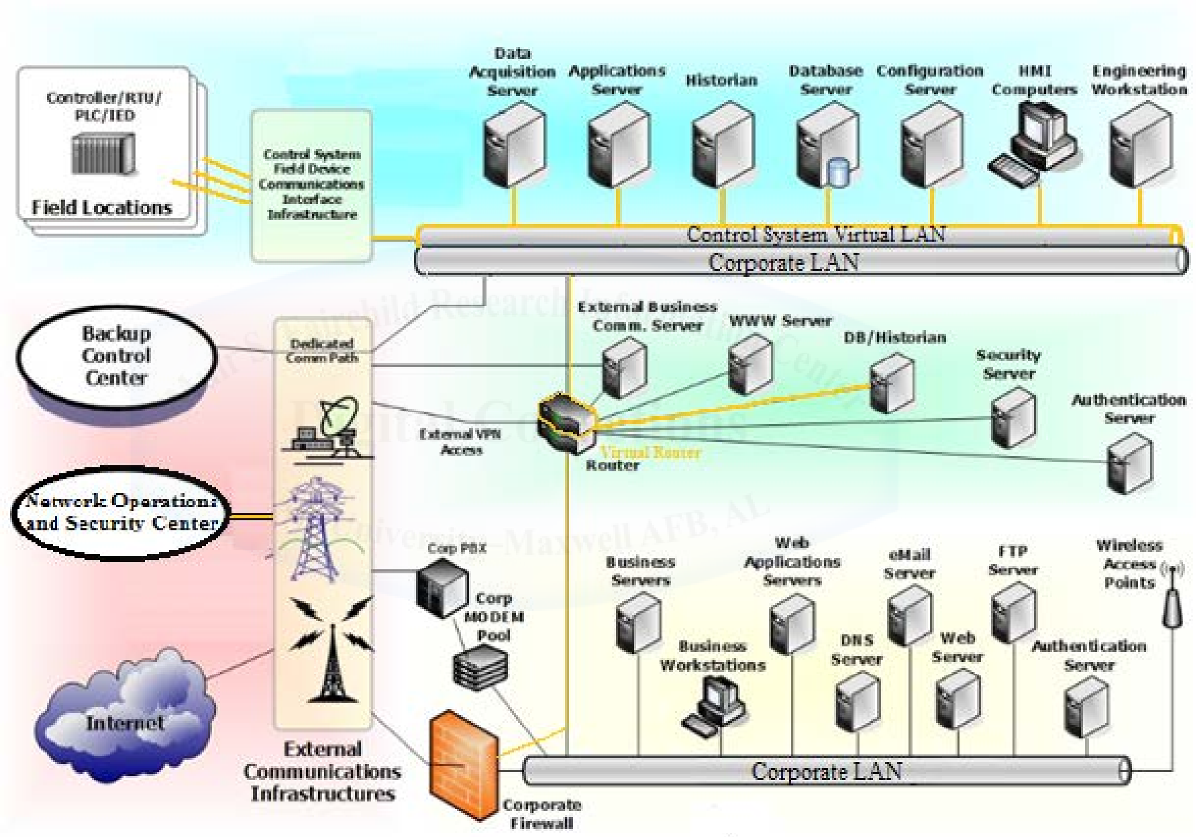


Figure 8: Logically Isolated Enterprise Architecture (Adapted from David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” [United States: Department of Energy, 2006]: 6.)

Stand Alone Enterprise

The stand alone enterprise for critical infrastructure cyber defense is similar to the stand alone network alternative in that no connectivity exists between the corporate network and the critical infrastructure control system network, external VPN access is established through a router connected to the control system network and to several servers, and communication between the control system network and remote field locations requires the use of a dial-up modem pool combined with wireless access points because the control system local area network could not be physically extended to those locations. Common IT services such as email and web access are not available inside of the control system network because of isolation from the internet and the corporate network. A network operations and security operations team, separate from the corporate network operations and security operations team, remotely accesses and defends an enterprise of control system networks.

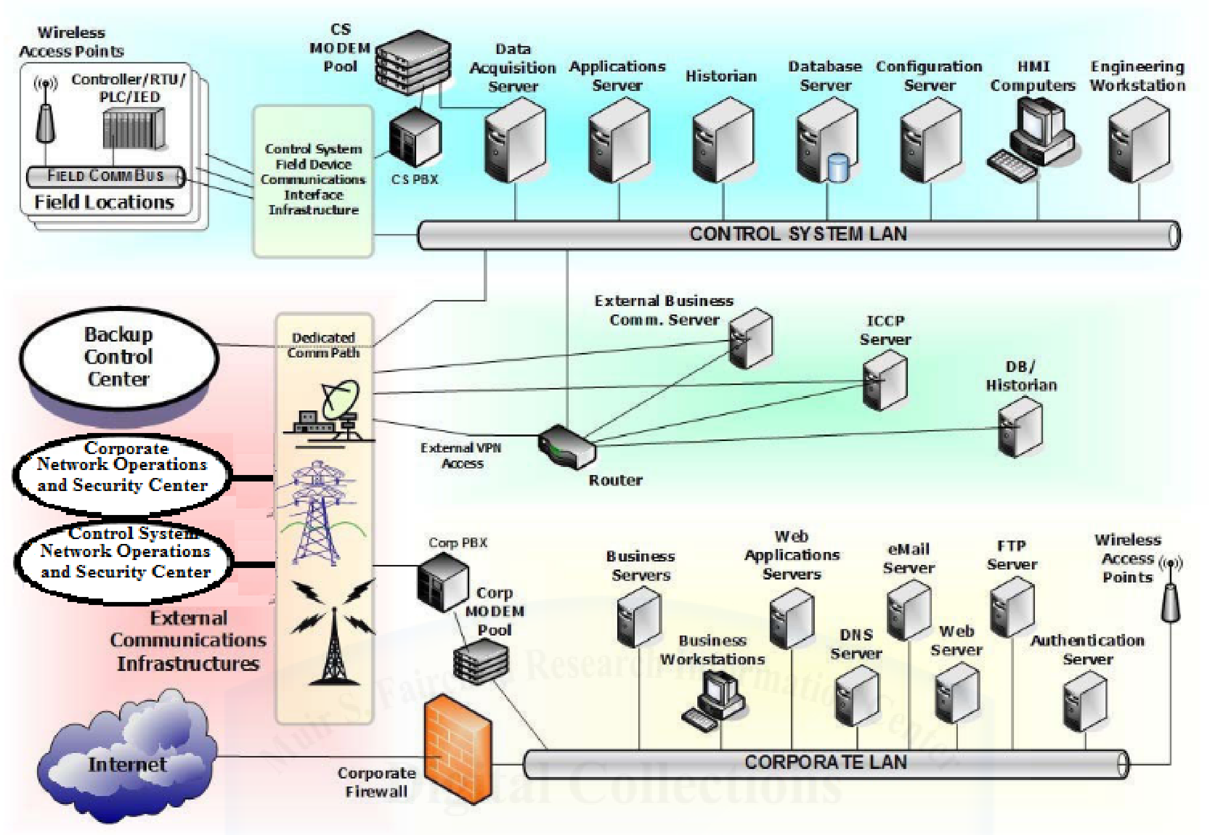


Figure 9: Stand Alone Enterprise Architecture (Adapted from David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” [United States: Department of Energy, 2006]: 4.)

V. Analysis of Alternatives

Five alternatives to critical infrastructure cyber defense were described in Section IV: the stand alone network, the Converged network, the logically isolated enclave, the logically isolated enterprise, and the stand alone enterprise. Each of these alternatives, as described in section IV, are evaluated using the critical infrastructure cyber kill chain aligned mitigation matrix developed in Section III (Figure 4) where, green indicates inclusion of a trait, blue indicates partial inclusion of a trait, and orange indicates a cyber defense trait is not accounted for in the alternative.

Stand Alone Network

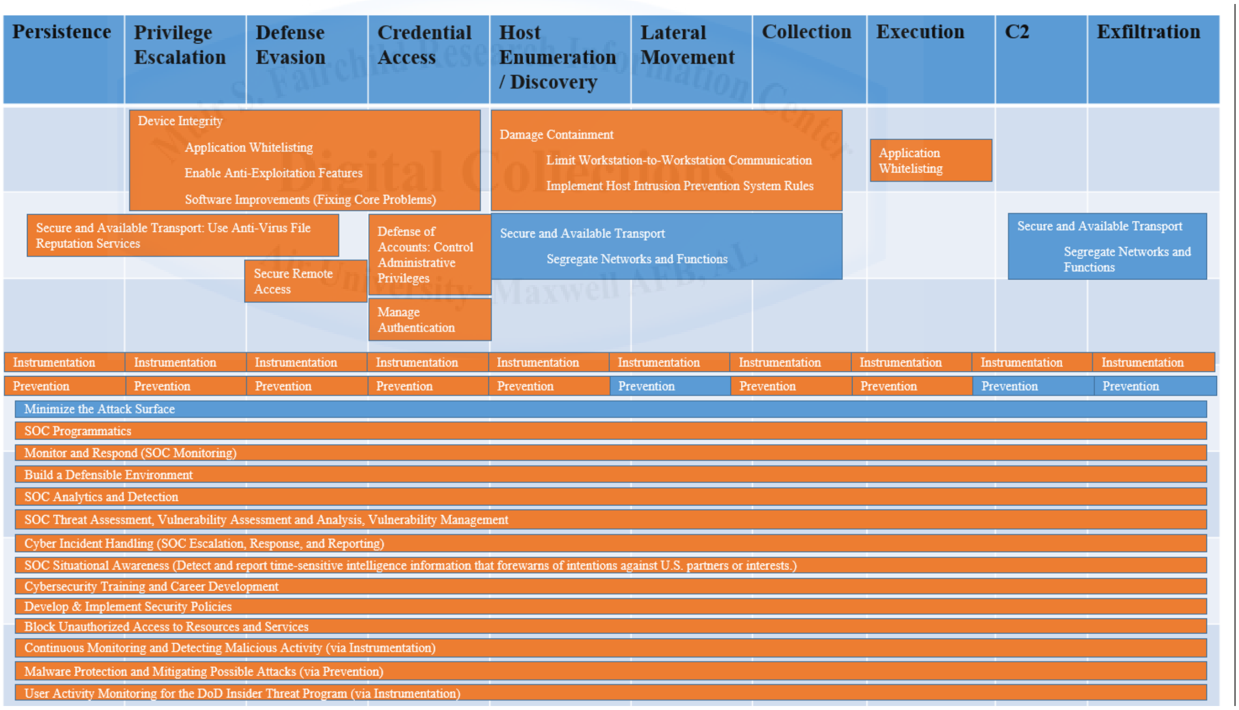

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Host Enumeration / Discovery
Lateral Movement
Collection
Execution
C2
Exfiltration
Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)
Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules
Application Whitelisting
Secure and Available Transport: Use Anti-Virus File Reputation Services
Defense of Accounts: Control Administrative Privileges
Secure and Available Transport
Segregate Networks and Functions
Secure and Available Transport
Segregate Networks and Functions
Secure Remote Access
Manage Authentication
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Instrumentation
Prevention
Prevention
Prevention
Prevention
Prevention
Prevention
Prevention
Prevention
Prevention
Prevention
Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 10: Criteria applied to Stand Alone ICS Alternative

In this alternative (Figure 10) no dedicated defenses or enterprise defenders exist. All cyber defense relies on physical isolation of the critical infrastructure's operational technology from other networks. External VPN access and modem access required to meet operational requirements limits the effectiveness of physical isolation.

Logically Isolated Enclave

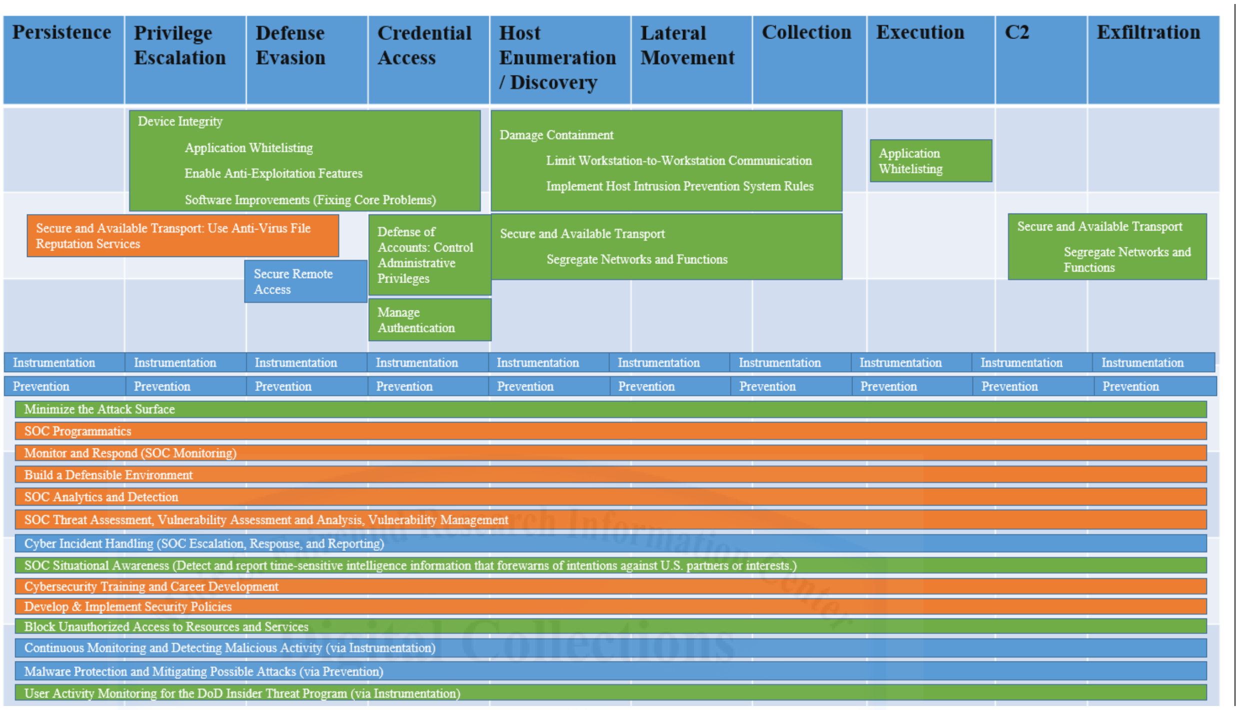

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Host Enumeration / Discovery
Lateral Movement
Collection
Execution
C2
Exfiltration
Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)
Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules
Application Whitelisting
Secure and Available Transport: Use Anti-Virus File Reputation Services
Defense of Accounts: Control Administrative Privileges
Secure and Available Transport
Segregate Networks and Functions
Secure and Available Transport
Segregate Networks and Functions
Secure Remote Access
Manage Authentication
Instrumentation
Prevention
Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 11: Criteria applied to Logically Isolated Enclave Alternative

The logically isolated enclave (Figure 11) uses network virtualization to benefit from IP network convergence while avoiding some limitations of the physically standalone system. A static defense is deployed inside of the logically isolated enclave which includes application whitelisting, central management of user accounts and administrative privileges. The modem network is replaced by the IP network increasing security of remote access. Operational requirements for remote access in an environment without network operations and security center control limit the effectiveness of this measure. The network operations and security operations team receives reports from the enclave which allows them to complete escalation and reporting of cyber incidents but would require a physical presence to perform a response.

Because the defenses implemented cannot be remotely updated by the security operations center, detection instrumentation and prevention capabilities are limited. This evaluation assumes the corporate cyber defense mitigates against compromise of network infrastructure.

Enterprise Networks

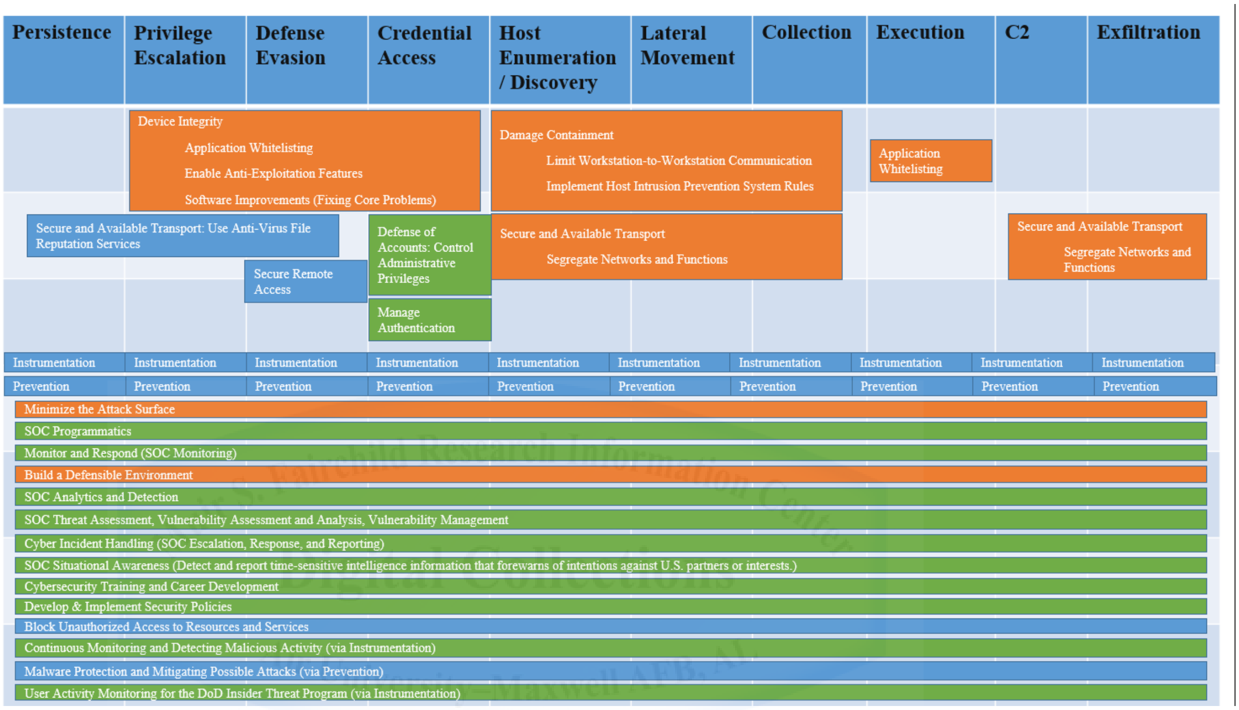

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Host Enumeration / Discovery
Lateral Movement
Collection
Execution
C2
Exfiltration
Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)
Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules
Application Whitelisting
Secure and Available Transport: Use Anti-Virus File Reputation Services
Defense of Accounts: Control Administrative Privileges
Secure and Available Transport
Segregate Networks and Functions
Secure and Available Transport
Segregate Networks and Functions
Secure Remote Access
Manage Authentication
Instrumentation
Prevention
Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 12: Criteria applied to Converged Enterprise Network Alternative

In this alternative (Figure 12), there is no differentiation by the network operations and security operations team between operational technology and information technology. As such, critical infrastructure specific mitigations such as application whitelisting and functional segregation of systems are not employed under this alternative. Instrumentation and prevention measures, as well as strict control of access to resources and services, are implemented but are not aware of their nature as operational technology. The network operations and security operations team is assumed capable of cyber defense of information technology in the corporate enterprise.

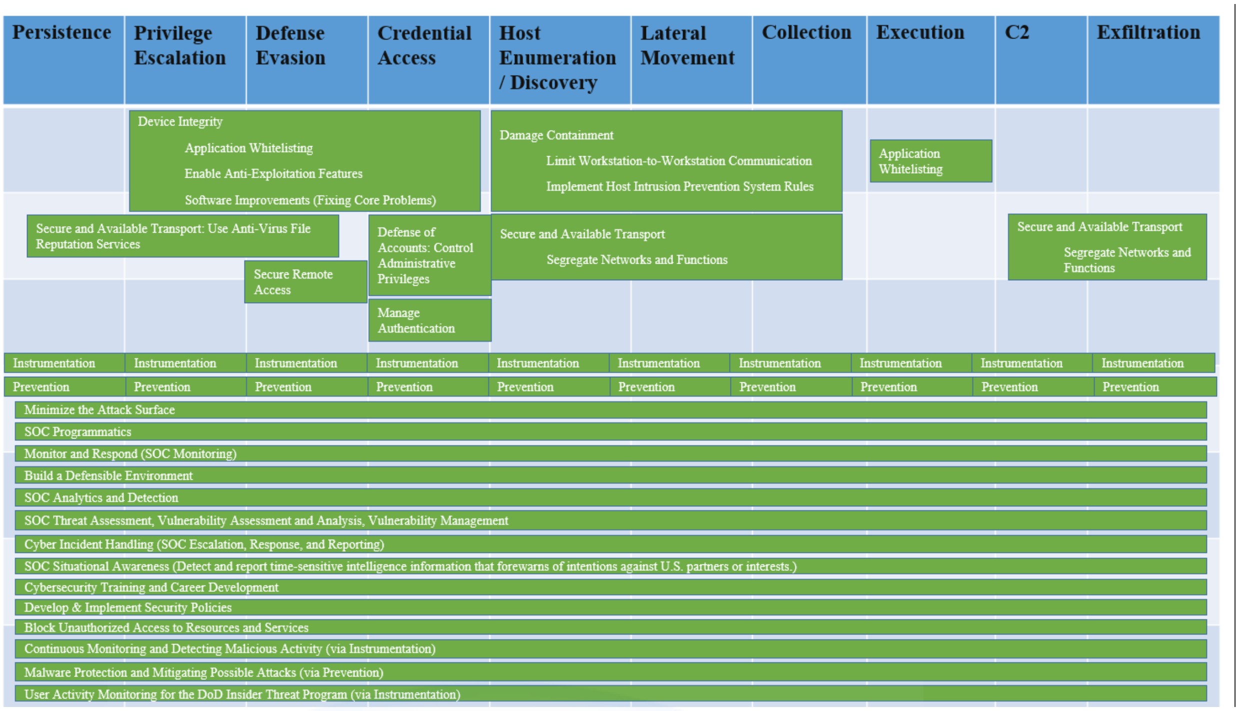

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Host Enumeration / Discovery
Lateral Movement
Collection
Execution
C2
Exfiltration
Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)
Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules
Application Whitelisting
Secure and Available Transport: Use Anti-Virus File Reputation Services
Defense of Accounts: Control Administrative Privileges
Secure and Available Transport
Segregate Networks and Functions
Secure and Available Transport
Segregate Networks and Functions
Secure Remote Access
Manage Authentication
Instrumentation
Prevention
Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 13: Criteria applied to Logically Isolated Enterprise Alternative

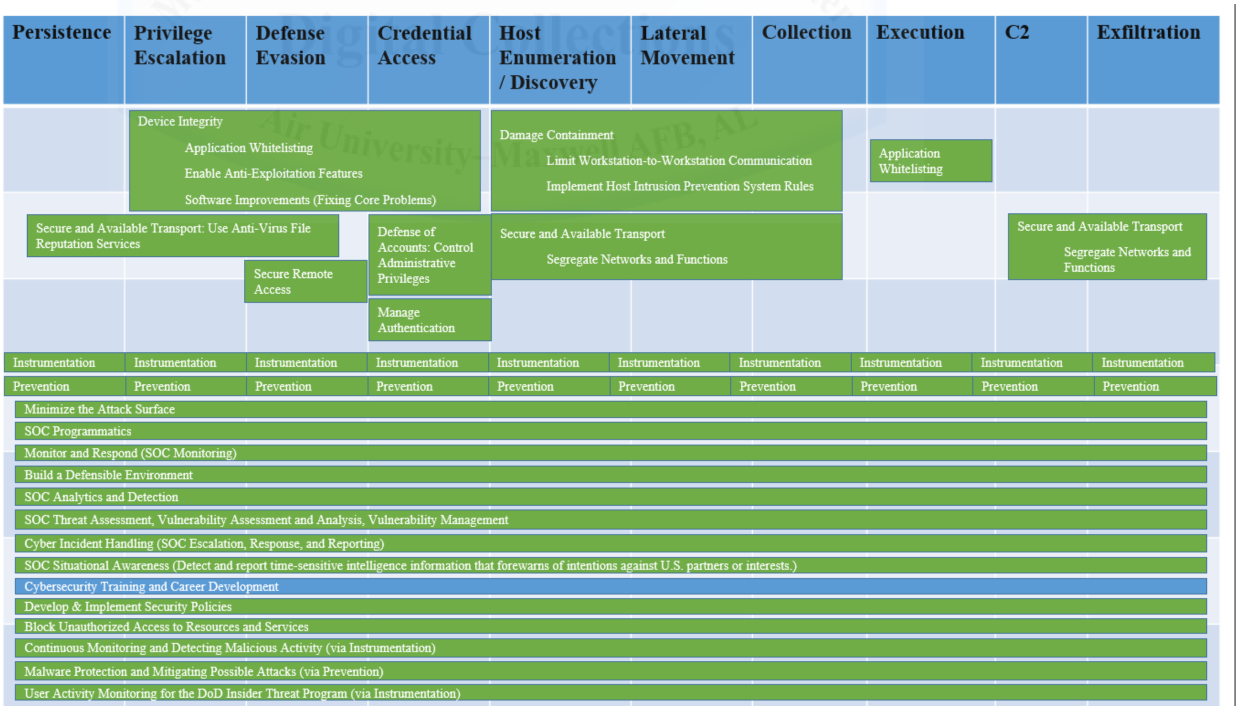

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Host Enumeration / Discovery
Lateral Movement
Collection
Execution
C2
Exfiltration
Device Integrity
Application Whitelisting
Enable Anti-Exploitation Features
Software Improvements (Fixing Core Problems)
Damage Containment
Limit Workstation-to-Workstation Communication
Implement Host Intrusion Prevention System Rules
Application Whitelisting
Secure and Available Transport: Use Anti-Virus File Reputation Services
Defense of Accounts: Control Administrative Privileges
Secure and Available Transport
Segregate Networks and Functions
Secure and Available Transport
Segregate Networks and Functions
Secure Remote Access
Manage Authentication
Instrumentation
Prevention
Minimize the Attack Surface
SOC Programmatics
Monitor and Respond (SOC Monitoring)
Build a Defensible Environment
SOC Analytics and Detection
SOC Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management
Cyber Incident Handling (SOC Escalation, Response, and Reporting)
SOC Situational Awareness (Detect and report time-sensitive intelligence information that forewarns of intentions against U.S. partners or interests.)
Cybersecurity Training and Career Development
Develop & Implement Security Policies
Block Unauthorized Access to Resources and Services
Continuous Monitoring and Detecting Malicious Activity (via Instrumentation)
Malware Protection and Mitigating Possible Attacks (via Prevention)
User Activity Monitoring for the DoD Insider Threat Program (via Instrumentation)

Figure 14: Criteria applied to Stand Alone Enterprise Alternative

There are few differences between the stand alone enterprise (Figure 14) and the logically isolated enterprise (Figure 13). Both alternatives include a network operations and security center with explicit programmatic authority and dedicated defenses to aid in the cyber defense of critical infrastructure. From the perspective of the standalone enterprise alternative, the most significant differences are the continued use of modems to extend the control system network to field locations and that the creation of a dedicated security operations team may limit career development opportunities for team members due to its specialized purpose. From another point of view, however, separating the control system network operations and security center from the corporate network operations and security center creates an opportunity to outsource the function which may be beneficial from a feasibility and resourcing perspective.

Discussion of the Results

The traditional cyber defense for critical infrastructure, the air-gap isolated and standalone system, has been shown lacking. Instead, the logically isolated enterprise network best meets the criteria derived through Section III. The use of existing IP networks as transport combined with expansion of existing capability in network operations and security centers appears to provide the best value; however, by duplicating both existing capability in the network operations and security center and expanding a standalone IP network to field locations the standalone enterprise alternative can match the capability of the logically isolated enterprise without being vulnerable to compromise of network infrastructure from the corporate network.

The converged enterprise network did surprisingly well against the developed criteria. With development of rules of engagement to prevent fratricide of operational technology and refinement of security operations center tactics, techniques, and procedures, it may be possible to develop the same level of expertise expected of the other two enterprise solution alternatives.

The logically isolated enclave alternative was found to provide a limited and static defense of the operational technology systems involved in critical infrastructure but was a significant improvement over the traditional standalone network. In monolithic organizations where the network operations and security operations teams cannot be readily reorganized to defend critical infrastructure this alternative becomes the most feasible and can be accomplished without expansion of existing capabilities. This approach can also be followed as a tactical solution for cyber key terrain, however, for long term defense of critical infrastructure an enterprise approach is better due to the convergence of mission assurance functions and classical computer network defense functions as identified in *Mission Assurance as a Function of Scale* and elaborated upon in section II.

VI. Recommendations

This study provides two recommendations. First and foremost, an enterprise approach to cyber defense of critical infrastructure should be selected and planning efforts initiated to implement the selected approach. Second, while no perfect solution is available for immediate implementation at zero cost, immediate measures to better defend critical infrastructure can and should be taken.

An enterprise approach to cyber defense of critical infrastructure is necessary to the establishment of Security Operations Center related capabilities. Security Operations Center related capabilities included: Monitoring and Response, Analytics and Detection, Threat Assessment, Vulnerability Assessment and Analysis, Vulnerability Management, Cyber Incident Handling, Cybersecurity Training and Career Development, Development & Implementation of Security Policies, Blocking Unauthorized Access to Resources and Services, Continuous Monitoring and Detecting Malicious Activity, Malware Protection and Mitigation of Possible Attacks, and User Activity Monitoring. Implementation of these capabilities requires the hire of numerous cybersecurity professionals on a scale that is not practical to duplicate on a per-system basis across the Air Force.

Defenses deployed by local system owners and cyber protection teams are better than nothing. The team can jerry-rig the capabilities of a functional Security Operations Center localized to a small number of mission essential critical infrastructure systems for the duration of that cyber protection team’s mission. This approach provides mission assurance to a specific mission but foregoes the opportunity provided by long term cyber defense activities to baseline normal activity and opportunities to prevent threat actor activities ranging from reconnaissance to establishing persistence through malware infection. Interdependency of the defended critical infrastructure upon other, undefended, critical infrastructure reduces, but does not completely eliminate, the effectiveness of localized solutions. Enclave level network isolation and segmentation is not a perfect solution but is available for immediate implementation at zero cost and, as an immediate measure to better defend critical infrastructure, it can and should be taken.

VII. Conclusion

Based on criteria derived from Department of Defense doctrine, commercial best practice, and recommendations from the Department of Homeland Security and the National Security Agency, this study has found that the pursuit of a Logically Isolated Enterprise provides the best solution for cyber defense of critical infrastructure. Research by Trepagnier and Schulz showed that short term mission assurance of specific cyber key terrain is meaningful but that over long periods of time and for large networks, such as the network formed by critical infrastructure interdependency, mission assurance of cyber key terrain converges with more traditional enterprise network defense. As such, for short term mission assurance of specific cyber key terrain, creation and defense of a Logically Isolated Enclave can be accomplished immediately and with near zero cost by a Cyber Protection Team but long term mission assurance still requires an enterprise solution for cyber defense of critical infrastructure. Cyber key terrain is a relatively new concept and this research may need to be revisited after the field is more mature. This study was limited in its ability to address all stakeholders associated with critical infrastructure. Despite having limitations this study has some implications for the Air Force.

Bibliography

Ashton Carter, "The DoD Cyber Strategy," (Washington, DC: Department of Defense, April 2015)

Barack Obama, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," (Washington, DC: February 2013)

Carson Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," (MITRE, October 2014)

C P Pfleeger and S L Pfleeger, “Security in Computing. 3rd ed.” (NJ: Prentice Hall, 2003)

David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” (United States: Department of Energy, 2006)

David Mussington, “Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development.” (Santa Monica, CA: RAND Science and Technology Institute, 2002)

Department of Defense Instruction 3020.39, Mission Assurance Policy for the Defense Intelligence Enterprise (DIE), (Washington, DC: Department of Defense, 2 March 2015)

Department of Defense Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, (Washington, DC: Department of Defense, 24 May 2016)

Department of Defense, "Quadrennial Defense Review Report 2010," (Washington, DC: Department of Defense, January 2010)

Department of Defense, "Quadrennial Defense Review Report 2014," (Washington, DC: Department of Defense, March 2014)

Department of Defense Computer Security Center. “DoD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria.” (Washington, DC: Department of Defense, December 1985).

Department of Homeland Security, Critical Infrastructure Sectors, (27 October 2015)

Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research Volume 1, (Academic Conferences Limited, 2011)

George J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter." (AFCEA, 14 August 2012)

Harry Harris and William Gortney, Letter on ICS Cybersecurity to the Honorable Ash Carter Secretary of Defense, (11 February 2016)

ICS-CERT, Seven Steps to Effectively Defend Industrial Control Systems, (Idaho Falls, Idaho: 2016)

Information Assurance Directorate, Top 10 Information Assurance Mitigation Strategies, (Washington, DC: National Security Agency, 2015)

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. (15 February 2016)

Joint Publication 3-12, Cyberspace Operations, (Washington, DC: Department of Defense, 5 February 2013)

Joint Publication 6-0, Joint Communication System, (Washington, DC: Department of Defense, 10 June 2015)

Keith A. Stouffer, Joseph A. Falco, and Karen A. Scarfone. "SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)." (Washington, DC: NIST, 2011)

Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security," (Washington, DC: Department of Defense, October 2012)

Michael Chipley, Cybersecurity, (Whole Building Design Guide, June 2016)

Microsoft, "The STRIDE Threat Model," (Microsoft, 2005)

Peter Pace, "National Military Strategy for Cyberspace Operations (NMS-CO)," (Washington, DC: Joint Chiefs of Staff, 2006)

Peter Pederson, D. Dudenhoeffer, Steven Hartley, and May Permann, "Critical infrastructure interdependency modeling: a survey of US and international research." (Idaho National Laboratory, 2006)

Pierre Trepagnier and Alexia Schulz, "Mission Assurance as a Function of Scale," (MIT: Lincoln Laboratory, 2015)

Protiviti Inc, Managing Risks in Operational Technology Systems, (2013)

Rae Zimmerman, "Understanding the implications of critical infrastructure interdependencies for water," (CREATE Research Archive, March 2009)

Stallings W, “Cryptography and Network Security-Principles and Practices. 4th ed.” (Pearson Education, 2006)

Steffi Haag and Andreas Eckhardt, "Justifying Shadow IT Usage," Proceedings of the 19th Pacific Asia Conference on Information Systems, (Singapore, SG: Association for Information Systems, July 2015)

Steven Alter, "Theory of workarounds," Communications of the Association for Information Systems, Vol. 34, Article 55, (San Francisco, CA: University of San Francisco, 2014)

The MITRE Corporation, "ATT&CK," (The MITRE Corporation, 20 May 2015)

The White House, “National Strategy to Secure Cyberspace,” (Washington, DC: The White House, 2003)

Trey Herr, "PrEP: A framework for malware & cyber weapons," The Journal of Information Warfare, (Cambridge, MA: Harvard Kennedy School, 20 December 2013)

U.S. ARMY CORPS OF ENGINEERS, UFGS-25 10 10, November 2015.

Zhang H G, Wang L N, Huang C H, Research and practice for information security discipline construction and personnel training, Symposium on Deans of Computer Institute of China (Beijing: Higher Education Press, 2005)

Endnotes

[1] Leon E. Panetta, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security,” (Washington, DC: Department of Defense, October 2012): http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

[2] Peter Pace, “National Military Strategy for Cyberspace Operations (NMS-CO),” (Washington, DC: Joint Chiefs of Staff, 2006): 14.

[3] Peter Pace, “National Military Strategy for Cyberspace Operations (NMS-CO),” (Washington, DC: Joint Chiefs of Staff, 2006): 13.

[4] The White House, “National Strategy to Secure Cyberspace,” (Washington, DC: The White House, 2003): vii.

[5] The White House, “National Strategy to Secure Cyberspace,” (Washington, DC: The White House, 2003): viii.

[6] Department of Defense, "Quadrennial Defense Review Report 2010," (Washington, DC: Department of Defense, January 2010): x.

[7] Department of Defense, "Quadrennial Defense Review Report 2014," (Washington, DC: Department of Defense, March 2014): 7.

[8] Department of Defense, "Quadrennial Defense Review Report 2014," (Washington, DC: Department of Defense, March 2014): 15.

[9] Ashton Carter, "The DoD Cyber Strategy," (Washington, DC: Department of Defense, April 2015.): 10.

[10] Barack Obama, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," (Washington, DC: February 2013): https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[11] Department of Homeland Security, *Critical Infrastructure Sectors*, (27 October 2015): https://www.dhs.gov/critical-infrastructure-sectors

[12] Zhang H G, Wang L N, Huang C H, *Research and practice for information security discipline construction and personnel training*, Symposium on Deans of Computer Institute of China (Beijing: Higher Education Press, 2005); C P Pfleeger and S L Pfleeger, “Security in Computing. 3rd ed.” (NJ: Prentice Hall, 2003); Stallings W, “Cryptography and Network Security-Principles and Practices. 4th ed.” (Pearson Education, 2006); Department of Defense Computer Security Center. “DoD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria.” (Washington, DC: Department of Defense, December 1985).

[13] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. (15 February 2016): 135.

[14] George J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter." (AFCEA, 14 August 2012): 7, http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf

[15] Department of Defense Instruction 3020.39, Mission Assurance Policy for the Defense Intelligence Enterprise (DIE), (Washington, DC: Department of Defense, 2 March 2015): 7.

[16] Department of Defense Instruction 3020.39, Mission Assurance Policy for the Defense Intelligence Enterprise (DIE), (Washington, DC: Department of Defense, 2 March 2015): 7.

[17] Peter Pederson, D. Dudenhoeffer, Steven Hartley, and May Permann, "Critical infrastructure interdependency modeling: a survey of US and international research." (Idaho National Laboratory, 2006): 9.

[18] Harry Harris and William Gortney, Letter on ICS Cybersecurity to the Honorable Ash Carter Secretary of Defense, (11 February 2016): 1.

[19] Joint Publication 3-12, Cyberspace Operations, (Washington, DC: Department of Defense, 5 February 2013): III-2.

[20] Steffi Haag and Andreas Eckhardt, "Justifying Shadow IT Usage," Proceedings of the 19th Pacific Asia Conference on Information Systems, (Singapore, SG: Association for Information Systems, July 2015): 4.

[21] Steven Alter, "Theory of workarounds," Communications of the Association for Information Systems, Vol. 34, Article 55, (San Francisco, CA: University of San Francisco, 2014): 1044.

[22] David Mussington, “Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development.” (Santa Monica, CA: RAND Science and Technology Institute, 2002): 29.

[23] Peter Pederson, D. Dudenhoeffer, Steven Hartley, and May Permann, "Critical infrastructure interdependency modeling: a survey of US and international research." (Idaho National Laboratory, 2006): 3.

[24] Pierre Trepagnier and Alexia Schulz, "Mission Assurance as a Function of Scale." (MIT: Lincoln Laboratory, 2015): 2.

[25] Michael Chipley, *Cybersecurity*, (Whole Building Design Guide, June 2016): https://www.wbdg.org/resources/cybersecurity.php

[26] Rae Zimmerman, "Understanding the implications of critical infrastructure interdependencies for water," (CREATE Research Archive, March 2009): 4.

[27] Pierre Trepagnier and Alexia Schulz, "Mission Assurance as a Function of Scale." (MIT: Lincoln Laboratory, 2015): 2.

[28] Joint Publication 3-12, Cyberspace Operations, (Washington, DC: Department of Defense, 5 February 2013): GL-4.

[29] Harry Harris and William Gortney, Letter on ICS Cybersecurity to the Honorable Ash Carter Secretary of Defense, (11 February 2016): 1.

[30] Joint Publication 6-0, Joint Communication System, (Washington, DC: Department of Defense, 10 June 2015): I-7.

[31] Department of Defense Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, (Washington, DC: Department of Defense, 24 May 2016): 27.

[32] Department of Defense Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, (Washington, DC: Department of Defense, 24 May 2016): 27.

[33] U.S. ARMY CORPS OF ENGINEERS. UFGS-25 10 10. November 2015. 78.

[34] Department of Defense Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, (Washington, DC: Department of Defense, 24 May 2016): 27.

[35] Joint Publication 6-0, Joint Communication System, (Washington, DC: Department of Defense, 10 June 2015): I-7.

[36] Carson Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," (MITRE, October 2014): 44.

[37] Carson Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," (MITRE, October 2014): 307.

[38] Microsoft, “The STRIDE Threat Model,” (Microsoft, 2005): https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[39] Trey Herr, "PrEP: A framework for malware & cyber weapons," *The Journal of Information Warfare*, (Cambridge, MA: Harvard Kennedy School, 20 December 2013): 3, https://www.jinfowar.com/journal/volume-13-issue-1/prep-framework-malware-cyber-weapons.

[40] Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research Volume 1*, (Academic Conferences Limited, 2011): 5.

[41] The MITRE Corporation, "ATT&CK," (The MITRE Corporation, 20 May 2015): https://attack.mitre.org/wiki/Main_Page.

[42] ICS-CERT, *Seven Steps to Effectively Defend Industrial Control Systems*, (Idaho Falls, Idaho: 2016): 1.

[43] Information Assurance Directorate, *Top 10 Information Assurance Mitigation Strategies*, (Washington, DC: National Security Agency, 2015): 1.

[44] David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” (United States: Department of Energy, 2006): 4.

[45] David Kuipers and Mark Fabro. “Control Systems Cyber Security: Defense in Depth Strategies,” (United States: Department of Energy, 2006): 6.

[46] Protiviti Inc, *Managing Risks in Operational Technology Systems*, (2013): 2, https://www.protiviti.com/en-US/Documents/POV/POV-Managing-Risks-OT-Systems-Protiviti.pdf.

[47] Keith A. Stouffer, Joseph A. Falco, and Karen A. Scarfone. "SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)." (Washington, DC: NIST, 2011). 5-14.