

# THE DEPARTMENT OF DEFENSE'S NEW OPERATIONAL ENVIRONMENT: OT

---

A Thesis

Presented to

the Faculty of the Department of Information and Logistics Technology

University of Houston

---

In Partial Fulfillment of the

Requirements for the Degree

Master of Science Information

---

By

David Edwards

December 2018

# SIGNATURE PAGE

---

David E. Edwards

APPROVED

---

Christopher Bronk, PhD  
Committee Chair, Assistant Professor in  
Information and Logistics Technology Department

---

Wm. Arthur Conklin, PhD  
Associate Professor in  
Information and Logistics Technology Department

---

Denise M Kinsey, PhD  
Assistant Professor in  
Information and Logistics Technology Department

---

George Zouridakis, PhD  
Associate Dean for Research and Graduate Studies  
College of Technology

---

Enrique Barbieri, PhD  
Department Chair of Information and  
Logistics Technology

# ACKNOWLEDEMENT

I first want to thank my Lord and Savior, Jesus Christ for his grace and mercy. I live a blessed life and everyone I love and everything I have, I owe to Him.

None of this would have been possible without my loving wife, Sara Edwards, and two kids, Seychelle and Elijah Edwards. I am so thankful God gave them to me. Words cannot describe the love I have for my family.

To Sara, Seychelle and Elijah: Thank you for loving me.

To Anita and David: Thank you for raising me.

To Brittany and James Simpson: Thank you for inspiring me.

To Christian Ruiz: Thank you for always being there for me.

To Barrett Ward: Thank you for believing in me.

To Jon and Rachel Edelman, Sam and Maria Sobhani, Zan and Billi Morningstar: Thank you for putting up with me.

To Jay Anson, Thaddeus Underwood, David Southerland and Dr. Gilchrist: Thank you for mentoring me.

To Dr. Wm. Arthur Conklin, Dr. R. Christopher Bronk and Dr. Denise M Kinsey: Thank you for educating me.

# DISCLAIMER

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

# ABSTRACT

The purpose of this thesis is to outline how the Department of Defense (DoD), through Cyber Command, can holistically incorporate the cybersecurity of both DoD and non-DoD critical infrastructure into its cyber operations framework.

The United States and the DoD rely on critical infrastructure for basic life support to both civilians and the Armed Forces members tasked with the defense of this nation. Critical infrastructure is made up of industrial controls systems that fall under the taxonomy of operational technology (OT). In the 2018 Cyber Strategy, the DoD has been charged with defending both DoD and non-DoD critical infrastructure in a more aggressive posture to “defend forward.” To do this, the DoD needs to incorporate cybersecurity of critical infrastructure into the DoD’s holistic cybersecurity plan. However, the DoD has yet to address who will assume this mission, and how it will be accomplished. This research seeks to answer these questions and the reasons leading up to the DoD’s sudden change in policy.

# TABLE OF CONTENTS

## Chapter 1

1.1 Introduction.....	1
1.2 Problem Statement.....	2

## Chapter 2

2.1 Understanding Operational Technology and Information Technology.....	3
2.2 Operational Technology Challenges.....	5
2.2.1 Historical Summary of Operational Technology.....	5
2.2.2 General Operational Technology Challenges.....	6
2.2.3 General Operational Technology Security Challenges.....	7
2.3 Security Concepts.....	9
2.3.1 The Purdue Model.....	9
2.3.2 Top 20 for ICS.....	12
2.3.3 Risk Assessments.....	13

## Chapter 3:

3.1 Historical Review of DoD Critical Infrastructure.....	17
3.1.1 Historical Overview.....	17
3.1.2 Analysis of Findings.....	21
3.2 Whose House.....	21
3.3 Current Situation.....	24
3.3.1 Crawl Phase.....	24
3.3.2 Walk Phase.....	25
3.3.3 Run Phase.....	26
3.3.4 DoD Organizational Structure.....	27

## Chapter 4:

4.1 Designated Authority.....	29
4.2 Cyber Command Initial Challenges.....	31
4.3 Internal Challenges.....	31
4.3.1 Privatization of Critical Infrastructure.....	32
4.3.2 Standardization Across The Armed Force.....	32
4.3.3 Regulations and Policies.....	33
4.3.4 Uncoordinated Critical Infrastructure Updates.....	34

4.3.5 The Real Threat to DoD Critical Infrastructure.....	35
4.4 External Challenges.....	36
4.4.1 Information Sharing.....	37
4.4.2 Implementation of OT Security.....	37
4.4.3 Information Dissemination.....	38
Chapter 5:	
5.1 Advanced Persistent Threat: The STUXNET Dilemma.....	40
5.1.2 Flame.....	41
5.1.3 Duqu.....	42
5.1.4 STUXNET.....	43
5.1.5 The Olympic Games.....	46
Chapter 6:	
6.1 The Way Forward.....	49
6.1.1 Critical Infrastructure Protection Teams.....	49
6.1.2 Training.....	49
6.2 Sustains.....	51
6.2.1 Policy and Funds.....	51
6.2.2 Armed Forces.....	52
6.2.3 Partnerships.....	53
Chapter 7:	
7.1 Conclusion.....	57
Glossary of Abbreviations.....	60
References.....	63

# LIST OF FIGURES

Figure 2-1 Echelons of Critical Infrastructure.....	4
Figure 2-2 OT Security Principles.....	9
Figure 2-3 Purdue Model (Williams, 1989).....	10
Figure 2-4 Industrial Control System Risk Assessment Process (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).....	15
Figure 3-1 DoD Armed Forces and Combatant Command Structure.....	27

# LIST OF TABLES

Table 2-1 IT Security vs. Control System Security (Conklin, 2017).....	8
Table 2-2 Top 20 for ICS (Conklin, 2018).....	12
Table 2-3 Top 5 Risk Assessment Tasks (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017)....	14
Table 4-1 Uncoordinated Critical Infrastructure Updates.....	34
Table 5-1 STUXNET Zero-Day Attacks (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017)...	44



# CHAPTER 1

## 1.1 INTRODUCTION

On August 24<sup>th</sup>, 2012, General Ray Odierno was quoted “The strength of our nation is our Army. The strength of our Army is our soldiers. The strength of our soldiers is our families” (Odierno, 2012). The emphasis on the nation’s strength is outlined from the Army to the family. Yet so much of our national strength operates under the assumption that our critical infrastructure is available, operational, and secure. The world is entering a more complex future environment complicated by economic, military, and political uncertainty. Competition for resources, influence, wealth, and legitimacy generates unexpected and expected opportunists from nation-states, terrorist organizations, criminal organizations, hacktivist and other threat agents (Odierno, 2012). Threat agents are creating an asymmetric strategic environment, exploiting the information domain through innovative uses of computer technology. The information age has become a data-hungry environment. The need for real time data has extended to the United States’ critical infrastructure. The Patriot Act defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (DHS, 2015). Our critical infrastructure is run by Operational Technology (OT) that is susceptible to attack by threat agents looking to exploit vulnerabilities in our industrial control system. In order for the United States to maintain a competitive advantage, it is imperative that the DoD adapt to protect the nation’s critical infrastructure.

## 1.2 Problem Statement

The cybersecurity of the nation's critical infrastructure is of national importance and has come under the spotlight in recent years due to the large threat impact it could have on the safety of the nation and its people. However, securing these aging industrial control system has proven to be difficult as Information Technology (IT) increasingly gets incorporated into the OT domain. Industrial control systems running power, water, wastewater, and others use proprietary systems running legacy operating systems and protocols from the 1990s. In the early turn of the century, these control systems were exposed to the internet through an increasing demand for real-time information (Knapp & Langili, 2014). The high cost coupled with the inability to power down due to safety and/or environmental regulations makes updating critical infrastructure challenging (Conklin, 2016). The 2018 DoD Cyber Strategy states its responsibility to defend both DoD and non-DoD critical infrastructure as a top priority. Understanding industrial control systems, current security posture, and inherited vulnerabilities, are critical if the DoD is to defend it. The purpose of this thesis is to outline how the DoD, through Cyber Command, can holistically incorporate the cybersecurity of both DoD and non-DoD critical infrastructure into its cyber operations framework.

# CHAPTER 2

## 2.1 UNDERSTANDING OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY

The differences in goals, objectives, and security measures were taken in enterprises that utilize OT are different when compared to IT. IT is the study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information (Google, n.d.). OT is the hardware and software that monitor and/or control a physical process (Gartner, n.d.). In IT, the focus is on the protection of critical business information. IT is driven by data, whereas OT is driven by the operational capability of a system to control a process, and the protection of critical plant safety and productivity.

OT typically uses ladder logic and relay logic in its programmable logic controllers (PLC). Examples of OT range from air conditioners and garage doors to the industrial control systems in electric and nuclear facilities. Components found in OT for industrial control systems include remote terminal units, safety instrumented systems, intelligent electronic devices, human-machine interfaces, variable frequency drives, data historians, programmable automation controllers, and others (Conklin, 2016). These components work together to monitor and control actuators and sensors. Valves, pumps, motors and other equipment under control (EUC)/field devices, are used to regulate temperature, pressure, position, and levels to control a process. OT networks were once run with proprietary hardware and software not commonly known to others unless they had specific training and experience with that control system (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

For consistency and clarity in understanding critical infrastructure, operational technology and industrial control systems please refer to figure 2-1:

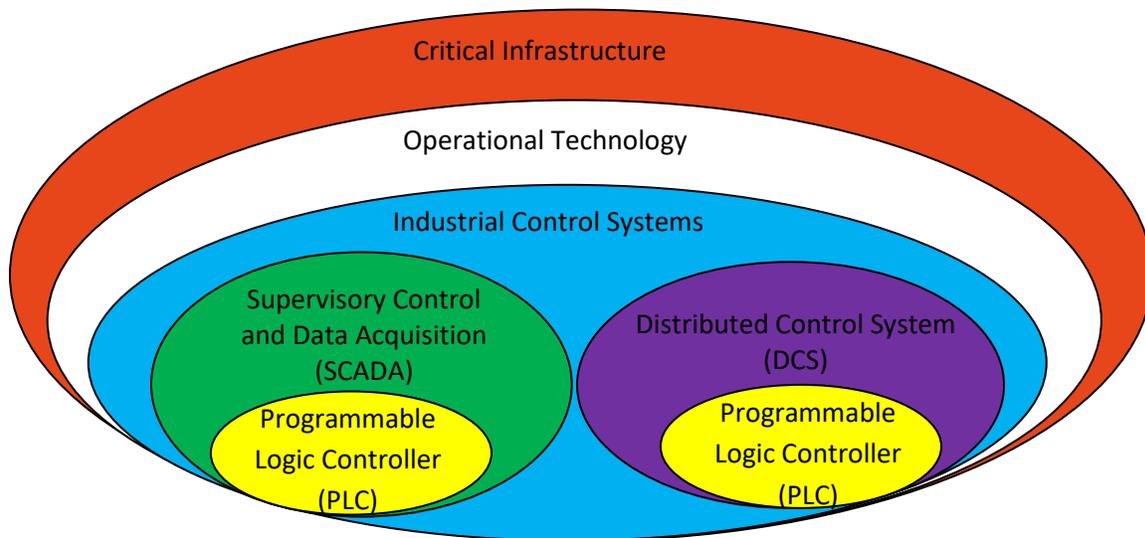


Figure 2-1 Echelons of Critical Infrastructure

Critical infrastructure refers to the industries that provide water, power, sewage, etc. Industrial control systems describe the technology used in critical infrastructure. When discussing industrial control systems, generally professionals refer to one of two main types of industrial control systems: Supervisory control and data acquisition (SCADA) and distributed control system (DCS). Both are control system architectures that use computers, networks, and human-machine interfaces for supervisory management (Conklin 2016). The difference lies in that SCADA provides centralized control functions for industrial control systems that are geographically dispersed and DCS distributes the control functions across a wide range of controllers that are generally contained within four walls (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). The term “control systems” are used in a general sense of OT specific automation and are found everywhere. A refrigerator would be an example of a control system. Industrial control systems are referring to control systems typically found in critical

infrastructure. An example of an industrial control system would be the United States' electric power grid which spans coast to coast and is the world's largest machine (Aggarwal, 2014).

## **2.2 OPERATIONAL TECHNOLOGY CHALLENGES**

### **2.2.1 Historical Summary of Operational Technology**

Industrial control systems started with PLC's, a digital computer adapted as high-reliability automation controller for industrial control systems (Conklin, 2016). PLCs started out as hardwired relay systems that could be updated in person, with a few hundred lines of code from a tape cartridge (Zetter, 2014). These first PLCs were first developed in the 1960s for the automotive industry (Pawar & Bhasme, 2016). The United States began seeing distributed control systems by Honeywell in the 1970s (Greenplant, 2011). Minicomputers and microprocessors replaced mainframes up through the 1980s (Conklin, 2016). Security concerns were limited due to the required intimate knowledge of the control system. In the 1990s, Congress passed environmental laws to regulate factory emissions. The Federal Energy Regulatory Commission (FERC) required the electric companies to monitor energy, output, and distribution. The need for up-to-date data and regulatory requirements pushed control system operators/owners to use commercial operating systems such as Microsoft and UNIX (Zetter, 2014). Thus the 1990s introduced the use of dial-up modems for remote connectivity to critical infrastructure. As OT systems and networks progress into the next century, the trend continues to move to open protocols, commercial off the shelf operating systems, and wireless (Conklin, 2016). Since the 1990s, industrial control systems have come under increased scrutiny concerning their security. The United States government has seen fit make critical infrastructure a priority in terms of national security.

### 2.2.2 General Operational Technology Challenges:

Providing security in OT is fraught with challenges on all fronts. Widespread implementation of Microsoft and UNIX operating systems in the OT environment has left the nation's critical infrastructure vulnerable to threats predominately seen in IT networks alone (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). OT systems run on operating systems that cannot be shut down for updates and patches because of environmental regulations and the negative impacts it can have on OT devices. Therefore, traditional cybersecurity best practices such as Microsoft Security Updates, antivirus, and patches are typically not done (Conklin, 2014). In addition, control system devices, protocols, and applications have not been inherently designed with security in mind, such as authentication, encryption, or other common countermeasures (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

A control system's primary focus is to strive for efficiency and reliability. OT protocols typically forgo any feature or function that is not absolutely necessary. Again, this includes security features like authentication and encryption which require additional overhead. Below provides a quick review of common control system protocols widely used in industry but should not be seen in IT networks. Those protocols are ModBus, DNP3.0, and ICCP.

**ModBus:** An open-source, messaging protocol often used between a supervisory computer and Remote Terminal Unit (RTU) (master-slave/client-server) and is commonly considered the de facto standard protocol for the control systems environment (ModBus, 2018). It is an application layer protocol and is used to communicate with simple devices. It uses only three Protocol Data Units (PDUs): Modbus request, Modbus response, and Modbus exception response (Knapp, 2018). If using Modbus, each device must be assigned a unique address as each command is addressed to a specific device or Modbus address. PDUs contain the Modbus address, function codes, and response/request to give the device-specific commands (Knapp, 2018).

**Distributed Network Protocol (DNP3.0):** Primarily used to send and receive messages between control system devices. DNP3.0 is an open-source, standards-based messaging

protocol. DNPs can be encapsulated in Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to enable RTU communications over IP based networks. This functionality enables DNP3.0 interoperability between master control stations and slave (outstations) for the electric utility industry (DNP 2012). DNP3.0 started out in electric but is now widely used in water, oil, and gas industries (DNP, 2012). It supports time-stamped and time-synchronized data for efficient and reliable real-time transmissions. DNP3.0 conducts cyclic redundancy checks (CRC) for data reliability (Knapp, 2018).

**Inter Control Center Protocol (ICCP):** An open-source, standards-based protocol designed for communication over wide area networks (WAN) between a utility control center and other (different) control centers, power plants, substations, etc. within the energy industry (Knapp, 2018). It enables many disparate control centers and facilities (like electric) to be able to communicate beyond the boundaries of individual utilities (Knapp, 2018). It can be and is used in load balancing between different electric companies. ICCP operates over any network protocol, including TCP/IP (Knapp, 2018).

OT is fundamentally different than IT. The ecosystem that drives OT vs IT causes security concerns for the nation's critical infrastructure. Identifying and understanding some of the basic OT concepts and protocols currently in use throughout industry will prove invaluable in accomplishing the DoD's mission in defending the nations critical infrastructure. However, this research paper in no way advocates for Cyber Command to take full ownership of securing industrial control systems, but rather to enhance the security and resiliency of owner and operator industrial control systems.

### **2.2.3 General Operational Technology Security Challenges:**

Broadly examining the table below, there is clearly a need to understand the disparity between IT (Information Systems Security) and OT (Control Systems Security) security standards.

Topic	Information Systems Security	Control Systems Security
Anti-virus& Mobile Code Countermeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-5 years	Up to 20 years
Outsourcing	Common/widely used	Rarely used
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24 x 7 x 365 x forever
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

Table 2-1 IT Security vs. Control System Security (Conklin, 2017)

The disparity in IT and OT security is readily apparent when comparing availability, support, patching, technology lifetime, and others addressed in table 2-1. These security topics are governed by principles used in both IT and OT networks. Cybersecurity in IT consists of three principle concepts (in order of priority): confidentiality, integrity, and availability- called CIA. IT defines confidentiality in terms of secrecy and unauthorized disclosure. Integrity is the assurance of the accuracy, reliability, and unauthorized modification of information. Availability is the access to data and resources by authorized individuals (Harris, 2013).

In OT, these principle security concepts must be redefined. In the OT ecosystem, these principle concepts are flipped, rather than CIA it is AIC. Availability takes priority, followed by integrity, and then confidentiality (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). However, AIC is not about data. Rather, availability relates to the safe access to control systems and

ensuring continuity of services produced by the control system. Integrity relates to the quality of data and the control of data flow in the control system. Historically, confidentiality was rarely considered in OT. With the onset of smart grids and IT and OT convergence, the importance of this security principle should increase. AIC together ensures a safe, reliable, and productive control system. Safety, reliability, and productivity are driven by policy, procedures, and people.

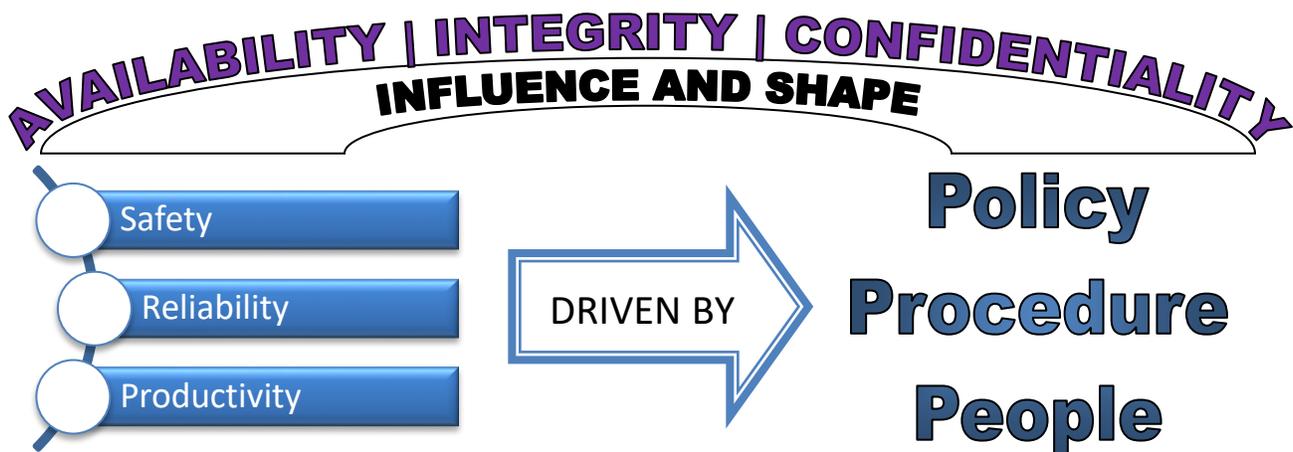


Figure 2-2 OT Security Principles

It is imperative for Cyber Command to understand the goals and objectives for OT security and how they integrate into that framework. To determine key security objectives, an OT cybersecurity professional must first determine the requirements. Ultimately, the requirements will drive policy. The policy must be specific to the control system. The system as designed, the system as deployed with a solution that can be controlled (Conklin, 2018).

## 2.3 SECURITY CONCEPTS

### 2.3.1 The Purdue Model:

The Purdue Model is the industry solution that achieves AIC and is seen as the most optimal method for organizing and controlling data flow of OT systems in a secure way. In a proof of concept, the Purdue Model is typically broken down into six layers, starting with layer

five, the enterprise layer, continuing to layer zero, the process area. For security reasons, industrial control facilities segregate their network into zones to control what goes into the OT network and what comes out. For simplicity, if Cyber Command were to operate in DoD and non DoD critical infrastructure, it would be in the enterprise security zone. The following Purdue Model offers a graphical representation of how security is logically organized:

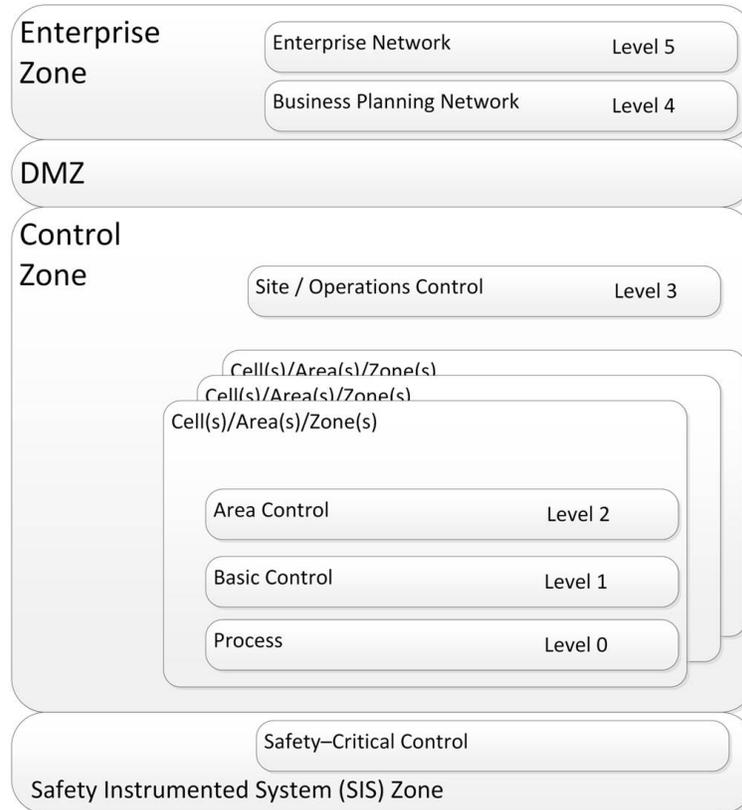


Figure 2-3 Purdue Model (Williams, 1989)

**Enterprise Zone, Layer 5:** The Enterprise Network Layer is comprised of typical software and hardware seen in IT ecosystems. These IT systems are used to govern multiple sites, Enterprises, or facilities that govern the overall supply and production generated by demand (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**Enterprise Zone, Layer 4:** In layer 4, facilities conduct business planning and logistics at the individual site. These are IT systems located at each individual site or facility that control the operation of that facility. Its primary function is to measure the performance against the production schedule (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**DMZ:** In-between layer 4 and layer 3 is the DMZ. The DMZ is a military term used in the industry that stands for demilitarized zone. The Purdue Model does not consider the

DMZ a separate layer. However, in an industrial control system DMZ, special equipment is used to separate and share information between the IT and OT Networks. Systems found in the DMZ include patch management servers, replication servers, engineering workstations, and change management systems. The purpose of this is to exchange critical information between the IT and OT networks without compromising the integrity, safety, and operation of the OT Network (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**Manufacturing Zone, Layer 3:** Layer 3 resides firmly in the OT side of the network. It has operator level interaction with the control system. Operators perform a supervisory role where process events are monitored (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**Supervisory LAN, Layer 2:** In layer 2, operators have local control over an individual area of a process. Operators use human-machine interfaces (HMI) to monitor and respond to alarms (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). HMI's give a graphical representation of the controlled environment to the operator and are used for control, monitoring, and alarming (Conklin, 2016).

**Basic Control or Controller LAN, Layer 1:** Basic control or Basic Process Control Systems (BPCS) is a generic term that references PLC, Variable Frequency Drives (VFD), sensors, actuators, relays and any other non-safety related control system used to control the process (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). VFD is a layer 1 device used to control the frequency and voltage applied to drives to manipulate their speed and direction of operation (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). Layer 1 devices are non-safety related control system controllers that receive input from EUC or field devices. (Ahmed, Naedele, Obermeier, & Richard, 2012).

**Bus Network or Process Area, Layer 0:** This layer focuses on equipment under control (EUC) from layer 1. (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). EUCs are individual field devices that are connected via a bus network (Ahmed, Naedele, Obermeier, & Richard, 2012). Examples are the drives, motors, valves, and other components in the PLC or VFD.

Finally, the Purdue Model outlines a safety layer. Depending on which version of the Purdue Model being referenced, the safety layer can be found in multiple areas, however, the safety layer is really incorporated in all layers of the Purdue Model to ensure the safety, reliability, and productivity of the control system. Ultimately the safety layer is responsible for mitigating anything that could result in the compromised availability and integrity of the

industrial control system. Compromised availability and integrity is defined in loss of view, control, or manipulation of the industrial control system (Conklin 2017). Typical components or devices found in the safety layer include interlocks and Safety Instrumented Systems (SIS). These safety devices are software or firmware encoded responses to a control system in an out of tolerance state. For example, SIS's are found in key areas of control systems to ensure the system brings the process to a safe state (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

### 2.3.2 Top 20 for ICS:

While the Purdue model is a way of logically organizing control processes in a secure way, Top 20 for ICS discusses the practical implementation of achieving AIC. It is originally derived from the Center for Internet Security top 20 controls implemented in IT ecosystems (CIS, 2018). Again, security principles must be redefined in OT. While the top 20 controls for IT may not be a 100% fit for OT, many of the same principles still apply. Influenced by the Center for Internet Security's top 20 controls, Dr. William A. Conklin, Associate Professor with the College of Technology with the University of Houston has a top 20 for industrial control systems.

1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4	Secure Network Engineering – enables the ability to control data flow (enclaves)
5	Limitation and Control of Network Ports, Protocols, and Services
6	Boundary Defense
7	Controlled Use of Administrative Privileges
8	Maintenance, Monitoring, and Analysis of Security Audit Logs
9	Security Skills Assessment and Appropriate Training to Fill Gaps
10	Incident Response Capability
11	Malware Defenses
12	Data Recovery Capability
13	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
14	Penetration Tests and Red Team Exercises

15	Controlled Access Based on the Need to Know
16	Account Monitoring and Control
17	Data Loss Prevention
18	Continuous Vulnerability Assessment and Remediation
19	Application Software Security – whitelist
20	Wireless Device Control

Table 2-2 Top 20 for ICS (Conklin, 2018)

Like IT, the first two controls are the same and are critical for an organization’s change management. Change management is the documented authorized changes to the network and/or system. This is crucial for IT ecosystems, where it can be complex and difficult to manage in larger organizations due to the short lifetime of equipment and software of about three to five years. However, due to the extended lifetime in OT, change management isn’t as complicated and a complete listing of all used hardware and software need to be accurate. Security professionals cannot secure a system or the software operating in OT if there is no accountability or documentation of it. As stipulated earlier, control systems are using legacy operating systems and devices with exceptionally long lifespans and thus critical that software and hardware are configured as safely as possible. Implementation of inherent security that is available provides a more layered defensive security regardless of how minimal. Controls four through eight segway into the Purdue Model’s domain and assist OT security professionals in engineering the control system in a logical, secure manner. Simply put, OT should be segmented as securely as possible from IT, while accounting for all deterministic data flows. While Top 20 for ICS controls seem elementary in thought, and seen as common sense, they are listed as a priority to address common security measures that are not being implemented.

Cyber Command is very familiar in operating in the IT domain, not in OT. The underline focus must be that in OT, nothing is more important than the safe, continued operation of a

system. Top 20 for ICS provides actionable guidance to making critical infrastructure more resilient.

### 2.3.3 Risk Assessments:

As most OT systems are specific in nature, it is difficult to have a commonly accepted risk metric for industrial control systems. Business objectives and operational environments are diverse, and defining risk metrics should be specifically tailored to the operating environment (Conklin, 2017). DoD critical infrastructure should balance mission needs, with functional and operational safety. Different DoD locations have various key assets with various levels of importance. Policies, procedures, and security controls should all be considered when developing feasible risk assessments. Industrial control system security professionals have listed 5 critical tasks:

1	Identify what needs to be protected.
2	Prioritize identified assets according to mission requirements and objectives.
3	Identify potential risks.
4	Measure the likelihood of occurrence and potential impact.
5	Security Controls are implemented based on the risks identified.

Table 2-3 Top 5 Risk Assessment Tasks (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017)

A proper risk assessment must be conducted to properly ascertain credible threats to DoD critical infrastructure. General security vulnerabilities and man-made disasters are a threat to OT. However, the DoD will need to incorporate advanced persistent threats from nation-states, terrorist, and others into their risk assessments. Attacker objectives will be different in OT than IT. In OT, the objective for an attacker revolves around three objectives: loss, manipulation, and denial. A loss of view, control, and safety. A manipulation of view, control and safety and finally the denial of view, control and safety (Conklin, 2018). A risk assessment flow chart for industrial control systems was developed by OT security professionals is outlined below.

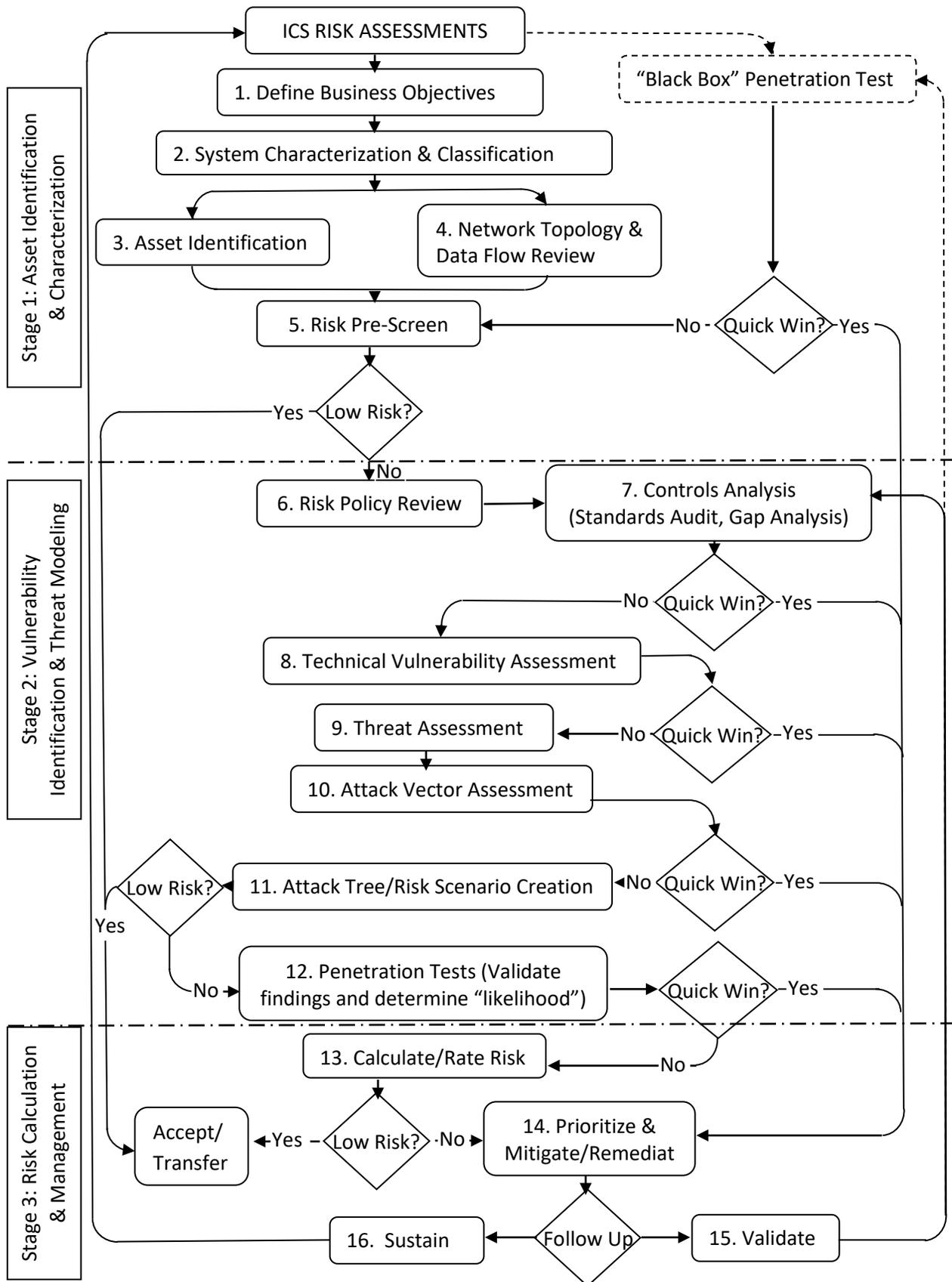


Figure 2-4 Industrial Control System Risk Assessment Process (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017)

Cyber Command needs to understand what drives security in OT, what best practices are exercised by industry, and to identify vulnerabilities in control systems. Having a firm understanding of the current situation will greatly assist Cyber Command in identifying and enforcing security standards, and develop a way forward. Outlined in figure 2-3, The Purdue Model helps to logically and physically organize data flow and is governed by the OT Security Principles seen in figure 2-2. Top 20 for ICS are best practices that identify what actions need to be taken by industrial control system security professionals. Again, these security measures should be conducted by industry. If anything, Cyber Command should be receiving and using risk assessment to identify where they can assist and enhance the defense of critical infrastructure and key assets of national interest.

# CHAPTER 3

## 3.1 HISTORICAL OVERVIEW OF DOD CRITICAL INFRASTRUCTURE

Before the DoD takes a more active role in OT across the nation, a good place to start would be its own backyard. A historical overview of key dates and events that pertain to the cybersecurity of the nation's critical infrastructure will provide the reference material needed to address the DoD's involvement in critical infrastructure. The idea of securing our nations critical infrastructure has been an ongoing concern for a few decades, but a focus to address the DoD's involvement in critical infrastructure is relatively new.

### 3.1.1 Historical Overview:

- 1998 **Presidential Decision Directive 63 (PDD-63):** The President of the United States established a directive to protect the nation's critical infrastructure. The PDD-63 identified nine sectors that are essential to the government operations and economic stability and assigned various lead agencies for each sector (PPD-63, 1998). The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism was assigned to lead this coordinated effort (Martin, 2006).
- 1998 **International Electrotechnical Commission (IEC) 61508:** An International Standard published by the International Electrotechnical Commission. IEC 61508 covers the functional safety of electrical/electronic/ programmable safety-related systems for EUC. In simple terms, the IEC 61508 brought awareness and guidance on standardization of functional safety to industrial control systems (IEC, n.d.).
- 1998 **Defense Reform Initiative #49:** Directed DoD Army and Air Force to privatize utility systems (DLA, n.d.).
- 1998 **Department of the Navy (DON) Critical Infrastructure Protection (CIP):** Secretary of the Navy Instruction 3501.1 formally established DON policy, structure, and responsibilities for implementing critical infrastructure protection throughout the Department of the Navy (Reiter, 2005).
- 2001 **09/11:** Terrorist organizations successfully plan an attack on the World Trade Centers in NYC and the Pentagon.

- 2001 **Executive Order 13231: Critical Infrastructure Protection in the Information Age.** Established the National Infrastructure Advisory Committee (NIAC). A collaboration between Federal, state, and private sector through a committee chaired by 30 people of influence in various critical infrastructure sectors. The intent is for increased collaboration, information sharing, incident coordination, and crisis response as it pertains to critical infrastructure (DHS, 2001).
- 2002 **The Homeland Security Act:** A direct result of the 09/11 terrorist attacks. The Homeland Security Act established the Department of Homeland Security (DHS) and created the Information Analysis and Infrastructure Protection Directorate, responsible for critical infrastructure protection (Martin, 2006). As of October 2018, there is no evidence to support that the directorate is still in operation. Last available reports are in 2004.
- 2003 **Homeland Security Presidential Directive 7 (HSPD 7): Critical Infrastructure Identification, Prioritization, and Protection.** HSPD 7 created the National Infrastructure Plan (NIPP) which aimed to unify critical infrastructure protection efforts across the country (DHS, 2015). HSPD 7 was a direct result of the 2002 Homeland Security act which gave the prime directive to identify and protect critical infrastructure and key resources (CIKR) (DHS, 2015).
- 2005 **The Energy Policy Act of 2005 (Energy Policy Act):** The Energy Policy Act established the Electric Reliability Organization (ERO), a self-regulatory organization with FERC oversight (NERC, 2012). FERC was given the authority to oversee the reliability and security of the power grid. FERC was also given the authority to approve mandatory cybersecurity reliability standards (CERC, 2018).
- 2006 **Section 215 of the Federal Power Act:** Requires that the ERO develop “mandatory and reliability standards, which are subject to FERC review and approval (NERC, n.d.).”
- 2006 **FERC Order 18 CRF Part 39:** An amendment to Section 215 of the Federal Power Act, the FERC developed a certification program outlining electric reliability standards the ERO must follow. These “reliability standards” outlined in Section 215 of the Federal Power Act include the cybersecurity protection of Bulk-Power Systems (NERC, 2006). Side note, this same year, NERC filed and was later approved to become the ERO (NERC, 2012).
- 2009 **The National Infrastructure Plan (NIPP):** Two key developments were borne out of the NIPP. The first was to leverage partnerships to enhance protection and resiliency and outline authorities, roles, and responsibilities for: federal, state, local, tribal, and territorial (SLTT), DHS, academia, private owners and operators of critical infrastructure. The other primary objective was to provide a Risk Management Framework to increase protection of CIKR. DHS assigned a critical infrastructure Protection Policy

- Coordination Committee to ensure coordination of policy relating to CIKR. However, it did not outline authority for DoD critical infrastructure. Only that the DoD participates in National Level Exercises responding to “all-hazards” environment to test NIPP protection plans (DHS, 2009).
- 2009 **DoDI 4170.11:** Mandated metering and energy load management on all DoD facilities. The intent was to reduce cost and leverage renewable sustainable energy (DoDI 4170.11, 2016).
- 2010 **American Recovery and Reinvestment Act (ARRA):** 14 billion dollars in grants and loans given by the government to push towards a nationwide deployment of smart-grid connected homes and companies (DOE, 2012). 7.2 billion dollars in grants and loans to expand broadband access (DOE, 2012).
- 2010 **STUXNET:** A small antivirus company named VirusBlockAda uncovered STUXNET, one of the most dangerous malware to ever be created. A malware aimed at industrial control systems (Zetter, 2014).
- 2012 **Presidential Policy Directive 21:** Loosely outlined resiliency and security roles and responsibilities of federal, SLTT, owners, and operators of critical infrastructure from cyber and physical threats. PPD 21 stipulated that General Services Administration (GSA) and DHS are to ensure contracts include security and resiliency audits for critical infrastructure (White House, 2012).
- 2013 **NIPP 2013: Partnering for Critical Infrastructure Security and Resilience:** Also known as the National Plan, the DHS updated the risk management framework from NIPP 2009 and set national priorities through information sharing and collaboration between government and industry coordinating councils. The DHS also stipulated that the DoD is to “operate, defend, and ensure the resiliency of DoD-owned or contracted critical infrastructure...” (DHS, 2013).
- 2014 **Air Force Civil Engineer Center-Air Force Cyber Nexus Collaboration (AFCEC-AFCYBER):** A collaboration agreement between the Air Force and industry to work together in strengthening the “security of industrial control systems that support critical Air Force infrastructures around the world” (Ausley, 2014).
- 2014 **U.S. Department of Energy Federal Building Metering Guidance:** The U.S. Department of Energy (DOE) was mandated by the President to meter Federal buildings for energy (electricity, natural gas, and steam) and water (DOE, 2014).
- 2015 **DoD Cyber Strategy:** Guidance issued by the DoD in developing cyber forces, strengthening the nations cyber defensive and deterrent posture. The Cyber Strategy annotates the importance of developing critical infrastructure resiliency through

partnerships with owners and operators. Defending the nation's critical infrastructure is not a top five priority (DoD Cyber Strategy, 2015).

- 2016 **Department of Defense Instruction (DoDI) 4170.11:** Further iterates privatization of utilities (electric, water, wastewater, and natural gas) provided to military installations. However, never defines any requirements for privatized utilities to provide security. This DoDI 4170.11 removes itself from a security focus to resiliency focus. The original stance in 2009 when DoDI 4170.11 was originally published clearly gave the DoD the responsibility to ensure the security of energy and water resources. Energy and water security were crossed out and replaced with "energy resilience" (DoDI 4170.11, 2016). DoDI 4170.11 defines Energy Resilience as "the ability to prepare for and recover from energy disruptions that impact mission assurance on military installations" (DoDI 4170.11, 2016). DoD installations are to "perform periodic vulnerability assessments and audits to assess the risk of energy disruptions on military installations, and implement remedial actions to remove unacceptable energy resilience risks" (DoDI 4170.11, 2016). Of note, the 2009 4170.11 gave the DoD the mandate to "...investigate off-base utility distribution and energy supply systems" (DoDI 4170.11, 2016). Ultimately 4170.11 assigns energy resilience to DoD components to ensure that DoD has available and reliable power to accomplish its missions from military installations and facilities (DoDI 4170.11, 2016).
- 2018 **Department of Defense Instruction (DoDI) 3020.45 (Mission Assurance Construct):** MA is defined as the ability to conduct all assigned tasks and duties as intended (DON CIP, 2009). DoDI 3020.45 establishes risk management requirements in identifying tactical and defense critical assets applicable to Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) to accomplish MA. DCI refers to the "composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide" (DoDI 3020.45, 2018). DIB refers to government or industry that provide research and development, and other critical components for the military (DoD Cyber Strategy, 2018).
- 2018 **Department of Defense Cyber Strategy:** Summary of DoD Cyber Strategy. Critical infrastructure becomes a top five objective for DoD. This strategy leapfrogs other publications in regards to critical infrastructure. "The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) entities" (DoD Cyber Strategy, 2018). The DoD is to accomplish this by "defend[ing] forward" outlined further in the strategy as "[t]he Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability" (DoD Cyber Strategy, 2018).

### **3.1.2 Analysis of the Findings:**

The United States slowly began to take the security of its critical infrastructure as a top national priority. Great lengths were taken to develop its stance on the cybersecurity of critical infrastructure and was a driving force in the development of a new federal organization, the DHS. While limited in capability due to critical infrastructure being privately owned, the DHS slowly began cultivating partnerships in the industry which brought about an increase in collaboration. As threats to critical infrastructure became more prevalent with a more interconnected critical infrastructure and the advent of highly sophisticated industrial control system malware, has led the DoD to become more involved in the defense of the nation's critical infrastructure. The 2018 Cyber Strategy takes a more offensive posture as the United States enters a more complex future environment. On the heels of the 2018 Cyber Strategy, an assessment of key organizations and agencies and their involvement in defending the nation's critical infrastructure is in order.

## **3.2 WHOSE HOUSE**

The Federal Government is composed of the Legislative, Executive, and Judicial Branches. Under the Executive Branch, the President oversees the Cabinet and independent federal agencies for the enforcement of federal laws (White House, n.d). The Cabinet is comprised of 15 executive departments. DHS is one of the 15 Cabinet Departments and is tasked with the protection of the nation's critical infrastructure. The DoD is another one of 15 departments. It is the largest agency and it is comprised of the Armed Forces, Defense Intelligence Agency, and the National Security Agency (NSA) (White House, n.d.). Per Cybersecurity Executive Order 13800: "It is the policy of the executive branch to use its

authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate" (White House, 2017). These agencies have officially been charged with the cybersecurity of the nation's critical infrastructure.

The influence of several government and non-government entities are revealed in the historical overview in the DoD involvement in the critical infrastructure. Over the past several decades, many organizations influenced the defensive posture of the United States critical infrastructure. While there are many organizations, outlined below are several key government entities that pertain to the security of the United States critical infrastructure.

**Department of Homeland Security:** The DHS has 14 Operational and Support Components. The DHS' National Protection and Programs Directorate is the component responsible for securing the nations critical infrastructure. Specifically the Office of Infrastructure Protection. Per HSPD7 in 2003, the DHS was officially charged with securing our nations critical infrastructure (DHS, 2015). Currently, the DHS has five core missions. Part of its mission is to reduce the vulnerability of critical infrastructure and key resources from terrorist attacks and other hazards. This is accomplished through managing risk via collaboration with public and private owners and operators of critical infrastructure. They provide guidance and a forum to freely exchange information to create national programs and policies on critical infrastructure security and resilience (DHS, 2016). National Cybersecurity and Communications Integration Center (NCCIC) and The Government Coordinating Council (GCC) is an exemplary product borne from the DHS objective of cross-collaboration. The GCC is a self-organized and self-governed council that is comprised of 16 key critical infrastructure sectors (DHS, 2018). What is important to note, is that the DHS is not charged directly with providing cybersecurity to critical infrastructure.

**Federal Bureau of Investigation (FBI):** The FBI's core mission is to handle domestic intelligence and security for the United States. The FBI has several programs that aid in the protection of critical infrastructure. A crime prevention program called InfraGard oversees the collaboration between just the FBI and owners and operators of critical infrastructure (InfraGard, n.d.). In a separate program, the FBI also partners with the DHS and private industry in the Domestic Security Alliance Council (DSAC). The DSAC is cross-collaboration between industry and the government to prevent, detect, and

investigate criminal acts as it pertains to interstate commerce, including critical infrastructure (DSAC, n.d.).

**General Services Administration (GSA):** The GSA provides acquisition support for all services, equipment, supplies, and IT to government organization and the military. This includes the construction and management of government-owned buildings. For DoD critical infrastructure, they align the acquisition process by developing common cybersecurity definitions, ensure any services or products meet the cyber risk management strategy and contracts meet the baseline cybersecurity requirements. (GSA, 2014) They also oversee the Office of Mission Assurance used to coordinate emergency management in the event of a national crisis, including a crisis involving critical infrastructure (DHS, 2015).

**Department of Defense (DoD):** Under the DoD is the Office of the Secretary of Defense which oversees the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (ODASD) and subsequently The Office of the Assistant Secretary of Defense for Energy, Installations, and Environment Installation Energy (ODASD(IE)). ODASD(IE) is responsible for the programs that manage energy and water for DoD installation in both the Continental United States (CONUS) and Outside the Continental United States (OCONUS) (ODASD(IE), n.d). They are not energy providers. Their purview includes policy, strategy, and the cybersecurity of DoD facility related control systems. Meaning, the cybersecurity of the energy used to heat, cool, and power DoD infrastructure. Infrastructure includes soldier barracks, office buildings, maintenance depots, and more (ODASD(IE), n.d). The ODASD defines cybersecurity of facility related control systems in terms of redundancy. Redundancy in energy capability enables energy resilience. DoD energy resilience is achieved by outlining the cost of life cycle energy solutions coupled with backup energy solutions to enable the military to fulfill mission requirements (Castillo, 2017).

**Defense Logistics Agency (DLA):** The Defense Logistics Agency provides supplies to the military services. As it pertains to control systems, the Defense Logistics Agency Energy awards and manages the contracts that handle privatizing defense utility systems including water, wastewater, power, and natural gas (DLA, n.d).

**National Security Agency (NSA):** The primary job of the National Security Agency is to collect foreign intelligence, synthesizing that data, and disseminate to appropriate leadership for action. Cybersecurity of United States communication networks and information systems (NSA, n.d.).

**National Institute of Standards and Technology (NIST):** Under the Department of Commerce, an executive department of the Cabinet, NIST releases Special Publications 800-53 and 800-82 to provide baseline security standards for the industrial control systems (Conklin, 2016). These publications assist in identifying typical threats and vulnerabilities along with recommended countermeasures for SCADA and DCS systems (Stouffer, Lightman, Abrams & Hahn, 2015).

**Federal Energy Regulatory Commission (FERC):** Regulates interstate transmission of natural gas, oil, and electricity, and audits NERC CIP preparedness against the risk of compromise to bulk electric systems (FERC, 2018). NERC CIP – Operates independently under the FERC. NERC CIP’s reliability standards regulate security within the North American bulk electric system. Bulk power systems are high-voltage transmission systems above 100kV and those that do not comply are levied with heavy penalties (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). Due to the 2005 Energy Policy Act, FERC can make cybersecurity reliability standards mandatory (FERC, 2018).

**Defense Information Systems Agency (DISA):** Under the DoD, DISA provides enterprise services via the Defense Information Systems Network to support the Armed Forces enabling Joint Operations (DISA, n.d.). Simply put, DISA is the gateway for the Armed Forces to the internet and the military’s secret network for both strategic and tactical networks (DISA, n.d.). The 2019 Defense Authorization Bill initially involved the closure of 27 agencies, DISA among them. It was later saved in an amendment supported by Democrats and the Pentagon (Mitchell, 2018).

## 3.3 CURRENT SITUATION

There is evidence to suggest that cybersecurity of critical infrastructure could have been better standardized throughout the DoD. Reviewing released publications concerning key organizations and the DoD’s progression through critical infrastructure history, a pattern begins to emerge. The United States defensive cybersecurity posture begins to display a crawl-walk-run pattern. The end result of the DoD taking a more definitive stance in their role of defending critical infrastructure may assist standardizing OT security across the DoD.

### 3.3.1 Crawl Phase:

In 1998, the Defense Reform Initiative pushed for the DoD to privatize its critical infrastructure. In 2002, the DoD’s ODASD(IE) released guidance for privatizing DoD utility systems. Per the DoD’s own guidance, all Defense Components will complete privatization both CONUS and OCONUS infrastructure unless they are exempted by mission requirements. The privatization of DoD critical infrastructure means that the DoD has no ownership of energy,

water, and other industrial control systems. “In order to effectuate privatization of the utility system, the Military Department must convey all rights in the asset” (ODASD(IE), 2002). No evidence was found that DoD still owned and operated its own critical infrastructure, but acknowledges that it does not make it true. However, the military has predominantly moved over to privatized utilities (DLA RFP, 2018). Thus for DoD critical infrastructure that has been privatized, there is no difference between industry and DoD owned critical infrastructure.

Released Presidential directives in 2002 gave the responsibility of defending the nation’s critical infrastructure to the DHS. In 2004, the DoD’s involvement was limited to DCI asset identification through the DoD Protected Critical Infrastructure Program (DCIP). This program was later rolled under the 2017 DoDI 3020.45 MA. Technically, a review of this time frame suggests that any critical infrastructure protection provided to DoD critical infrastructure would have fallen under the 2005 Energy Policy Act due to the privatization of DoD utilities. Interestingly, the DoD Armed Forces each saw its role in defending its critical infrastructure differently.

**The Department of the Army:** The largest of the Armed Forces, never stood up a program or organization to defend its critical infrastructure.

**The Department of the Navy:** The Navy immediately stood up the DON CIP the same year the DoD instructed all DoD utilities would be privatized in 1998 (Reiter, 2005). As of 2018, the DON CIP is still in effect.

**The Department of the Air Force:** In 2013 the DHS said that the DoD is responsible for securing DoD networks. A year later, the Air Force entered in AFCEC-AFCYBER agreement in 2014 (Ausley, 2014). This partnership with its privately owned critical infrastructure was done to collaborate a better defensive posture of Air Force critical infrastructure.

### 3.3.2 Walk Phase:

In 2016, the DoD released DoDI 4170.11 and definitively gave itself some measure of responsibility for “energy resiliency,” but not the defense. The defense of its critical

infrastructure was removed, yet the DoD still held the responsibility of performing vulnerability assessments and audits (DoDI 4170.11, 2016). No discrepancy is made in the DoDI 4170.11 between DoD owned critical infrastructure and privatized DoD critical infrastructure. In the energy sector, technically speaking, any standards or risk mitigation frameworks generated by NIST can be enforced by FERC for DoD's energy critical infrastructure (NERC, 2006) FERC and NIST collaborate to ensure that the incorporation of IT systems into OT architectures are implemented securely for all energy-specific control systems (FERC, 2018).

### **3.3.3 Run Phase:**

In 2018 the DoD released the 2018 Cyber Strategy and definitively declared its role in the defense of both DoD and non-DoD critical infrastructure. With the 2018 DoD Cyber Strategy clearly prioritizing the security of critical infrastructure as a top five priority, there is a clear shift in policy in the security of DCI. Security is redefined as the United States shifts focus from the 2015 Cyber Strategy. There is movement from building and developing our cyber force to conducting cyberspace operations that enhance U.S. military advantages. The defense of our critical infrastructure was defined in terms of resiliency through critical infrastructure partnerships and redundancy in energy infrastructure. Now the defense of our critical infrastructure is focused on the preemptive capability of stopping the malicious cyber activity. "Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident" (DoD Cyber Strategy, 2018).

To defend forward against any threat to our critical infrastructure, regardless of it having an impact on our warfighting readiness has bold implications. The question remains, what does this look like? Will a change in policy drive a more standardized approach to security DCI? Who in the DoD could support this mission? Analysis of the organization of the DoD, the

Armed Forces, and their respective cyber organizations will provide insight into how the DoD could conduct cybersecurity of its critical infrastructure.

### 3.3.4 DoD Organizational Structure:

The Unified Command Plan (UCP) and Combatant Commands are governed under Title 10 - Armed Forces; Subtitle A - General Military Law; Part I—Organization and General Military Powers; Chapter 6—Combatant Commands Section 161 – 168.

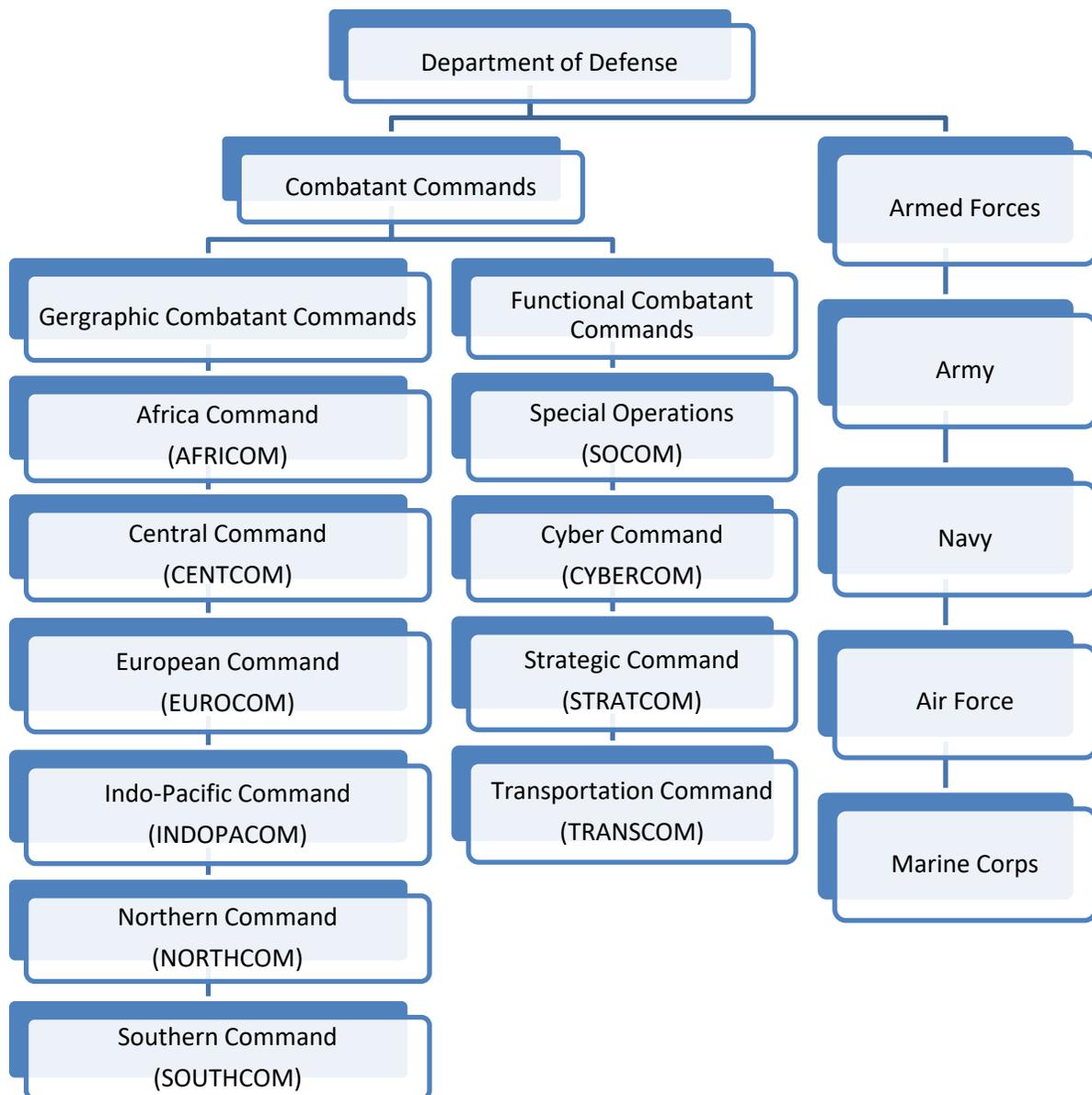


Figure 3-1 DoD Armed Forces and Combatant Command Structure

The DoD has many departments under it that are not listed in figure 3-1. While the DoD has yet to assign this mission to any particular agency, only a few candidates have the appropriate means to assume the mission to defend the United States critical infrastructure. While one option could be a defense agency, more plausible choices remain with the Armed Forces and Combatant Commands.

The DoD is tasked with providing military forces with the needs to deter war and ensure the nation's security (DoD, n.d.). The DoD's mission has extended to include the security of the United States critical infrastructure. To grasp the magnitude of this mission, a quick internal overview of just DoD owned assets is in order. Looking at just the Armed Forces, the DoD manages a worldwide real property portfolio valued at over \$705 billion (DMDC, 2017). 4,793 sites reside on 2.2 billion square feet of land. Of the 275,504 buildings, 23% have been privatized or operated by private entities (DMDC, 2017). The importance of this mission cannot be understated and the DoD will have to designate proper authority to the right agency or organization.

# CHAPTER 4

## 4.1 DESIGNATED AUTHORITY

DoD has several options in accomplishing its mission to defend the nations critical infrastructure. The first option involves the creation of a Defense Agency and/or Defense Field Activities. Typically defense agencies are used for supporting more than one military department when it is more economical or efficient (Cornel Law School, n.d.). Examples of Defense Agency's include DISA and the Defense Intelligence Agency's NSA. DISA is a possible option to assume this mission as DISA is a department under the DoD that provides tactical and enterprise services to the Armed Forces. However, DISA's mission and associated skillsets are too different to be a compatible fit for the cyber defense of OT. In an effort to save cost, the 2019 defense bill tried to eliminate DISA and other agencies through organizational changes. With an uncertain future, DISA does not seem a likely candidate to assume this role (Mitchell, 2018). Requirements for Defense Agencies and DoD Field Activities fall under the "combat support agency" under Title 10 (Cornel Law School, n.d.). The rhetoric used in the 2018 Cyber Defense Strategy hints at a more offensive posture and may need to extend past the restrictions outlined in Title 10 to ensure the security of the United States critical infrastructure. It is unlikely the DoD will have any Defense Agency assume the mission of protecting the nations critical infrastructure due to Title 10 limitations and compatible skillsets.

A quick review of figure 3-1 outlines the remaining organizational assets that the DoD can leverage short of standing up a new Combatant Command, or Armed Force. However, those are two of the four remaining options: stand up a Combatant Command, stand up a new Armed Force, assign this mission to a Combatant Command, or assign this mission to an existing

Armed Force. Of those four, it is unlikely that a new Combatant Command or Armed Force will occur to accomplish a singular mission. The 2019 defense bill was trying to eliminate and reorganize agencies in an effort streamline efficiencies and cut costs, standing up a new Combatant Command or Armed Force is the antithesis of what the House and Senate was trying to accomplish (Mitchell, 2018). Thus, the most likely course of action will be to assign this mission to a Combatant Command or Armed Force. Each Armed Force has a specific way of defending its critical infrastructure. There is little doubt that any Armed Force would want another Armed Force to secure their mission readiness. There is a reasonable assumption that a Combatant Command would assume this responsibility and each of the Armed Forces would support via a Service Component Command. The Combatant Command with the most compatible skillsets and proper jurisdiction would be Cyber Command. Within Cyber Command, a Joint Task Force could be set up to address this mission, as Joint Task Forces are often created to address a single policy concern.

Cyber Command has influence all over the world supporting Geographic Combatant Commanders. The current structure outlined in figure 3-1, was developed under the UCP. The UCP “establishes missions, responsibilities, and geographic area of responsibilities assigned to Geographic Combatant Commanders” (JP 3-0, 2018). Under the UCP, Cyber Command supports other Functional Combatant Commands and Geographic Combatant Commands with each Armed Forces cyber unit (CYBERCOM, 2018).

The Army Cyber Command supports Central Command, Africa Command, and Northern Command.

Air Forces Cyber supports European Command, U.S. Strategic Command, and U.S. Transportation Command.

The Fleet Cyber Command supports Pacific Command and Southern Command.

The Marine Corps Forces Cyberspace Command supports Special Operations Command (CYBERCOM, 2018).

Under this structure, Cyber Command is able to carry out the DoD's intent to "preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure..." on a global scale (DoD Cyber Strategy, 2018). Additionally as IT and OT integrate, skillsets found in Cyber Command will prove useful. Review of current trends and options available would lead to Cyber Command with each Armed Forces Cyber Service Component to assume this mission.

## **4.2 CYBER COMMAND INITIAL CHALLENGES**

Cyber Command is unfamiliar in this new operational environment. Offensively, Combatant Commanders and Cyber Command will most likely need reevaluate policy as it pertains to the forward defense and the rules of engagement. Clearly defined procedures in accordance with Combatant Command's authorized proper escalation of force. Defensively, Cyber Command needs to address glaring OT issues within the DoD.

## **4.3 INTERNAL CHALLENGES**

With a general understanding of challenges faced by OT systems in general, the DoD can begin to look at challenges within its organization. A few possible challenges faced by Cyber Command are discussed below.

#### **4.3.1 Privatization of Critical Infrastructure:**

As it stands, the 2018 Cyber Strategy calls for the defense of DCI. Which defines DoD critical infrastructure as both DoD and non-DoD assets that sustain military forces and operations worldwide (DoD Cyber Strategy, 2018). The DoD has privatized running power, water, wastewater, and other services (DoD, 2000). The new change in policy must take into consideration real property held by private industry, the contracts currently in place, and the effect on potential mission readiness and national security. The Department of the Army and Department of the Navy have made several attempts to mitigate this impact, but there is no standardization across the Armed Forces.

#### **4.3.2 Standardization Across The Armed Forces:**

With the possible exception of the Navy, the DoD has little experience in understanding how to secure OT systems. The Department of the Navy does have a critical infrastructure protection program whose mission is to ensure that both DoD and non-DoD critical infrastructure is available to meet the requirements of the Navy's MA. (DON CIP, 2009). While evidence suggests that the Navy actually runs its OT, it is not certain. The Air Force partnered with industry via the AFCEC-AFCYBER partnership (Ausley, 2014) while research suggests that the Army has no program at all. Multiple DoD publications and regulations such as the 2015 NIPP, 4170.11 and 3020.45 all discuss the importance of MA as it pertains to DoD critical infrastructure. Yet each of the Armed Forces displays varying degrees of involvement, which could lead to difficulty in standardizing policies and procedures among all three Armed forces.

### **4.3.3 Regulations and Policies:**

The ODASD(IE) is charged with the defense of the DoD facility related control systems (ODASD, 2017). The ODASD(IE) defines defense in terms of resiliency per 4170.11 and does not conduct actual cyber defense on OT systems that support DoD facilities. Thus a major factor in the DoD's plan to accomplish MA (outlined by DoDI 3020.45) of OT infrastructure supporting 700+ billion dollars in assets as was through energy resilience. Resilience achieved in redundancy in power capability (Castillo, 2017). When OT security is defined in terms of availability, integrity, and continuity, any over-reliance on one security principle over another can be just as dangerous. The integrity of OT cannot be achieved if there is no security measures taking place. The integrity of OT services is jeopardized by current DoD doctrine and regulations and thus must be updated. If not, money will continue to be spent by organizations under the DoD operating under the policy that defense is defined by availability and may no longer be in compliance with MA as defined by the 2018 Cyber Strategy.

In addition, the DoD has displayed a great deal of energy in ensuring the availability control systems for power, but there is little mention of other control systems, such as water, and wastewater in any regulation or policy.

#### 4.3.4 Uncoordinated Critical Infrastructure Updates:

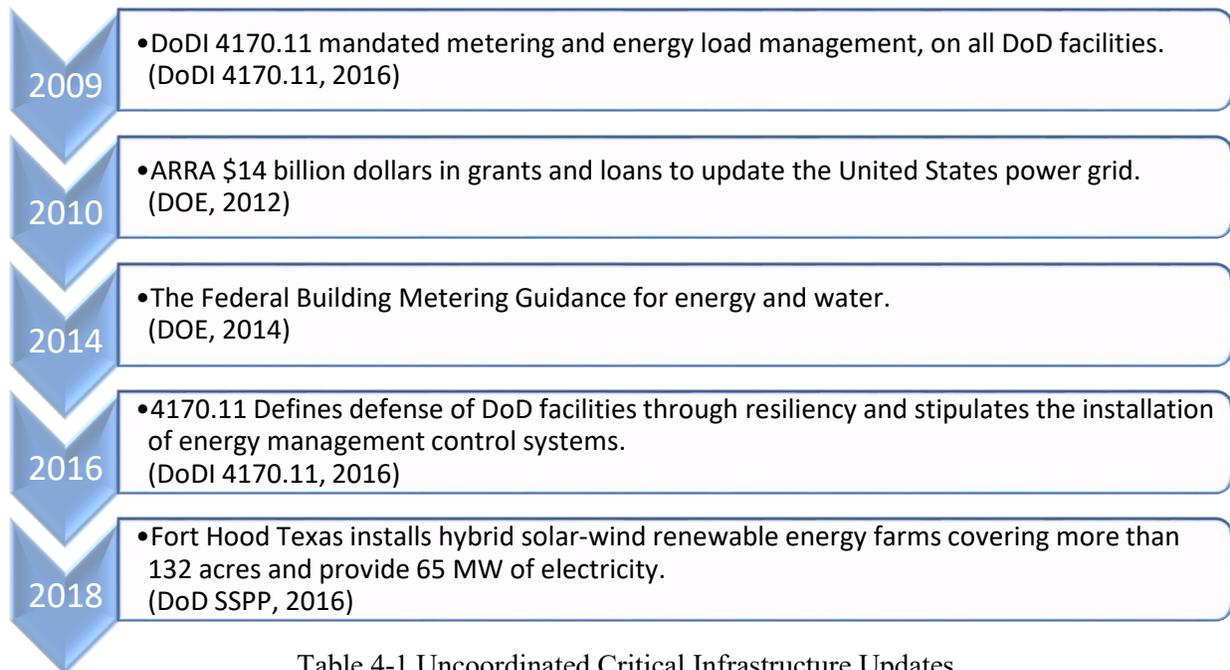


Table 4-1 Uncoordinated Critical Infrastructure Updates

The integrity of DoD critical infrastructure is further compounded as the United States government moves toward the smart grid and stipulates metered programs in an effort to reduce cost. IT convergence into OT infrastructure introduces more vulnerabilities without the cybersecurity infrastructure in place to ensure critical infrastructure is secure and reliable. A component of the smart grid is the smart meter. A feature of the smart meter is the ability to disconnect the user from the electric grid without having to send a technician (Zetter, 2010). In 2010, the ARRA pushed the United States towards the smart-grid without first ensuring that the technology was secure (Zetter, 2014). The 2014 Federal Building Metering Guidance stipulated that security should be used in the data centers that collect metered data from federal buildings, but nothing is mentioned about the security of the devices actually reporting the data from the control systems (DOE, 2014). The confidentiality of sensitive data relating to the DoD's energy use needs to be taken into account from end to end. Metadata related to power consumption of

DoD real property could unintentionally reveal sensitive information the DoD would rather be kept private.

While the threat from IT to OT is well documented, OT vulnerabilities also provide a pivot point for attackers into the IT. Exemplified in the Target breach in 2013, attackers pivoted from metered energy monitors used to reduce energy consumption by heating, ventilation, and air conditionings, or HVACs, from a third party company to Targets point-of-sale cash registers (Krebs, 2014). Attackers effectively stealing credit card information by gaining access to vulnerabilities in Targets OT network. If Kim Zetter is accurate about the lack of security in the United States governments push towards the smart grid, the potential for threat agents to leverage this vulnerability to gain access to DoD networks presents a legitimate security concern.

#### **4.3.5 The Real Threat to DoD Critical Infrastructure:**

Current evidence may suggest that the ODASD(IE) does not need to invest in the cyber defense of DoD facilities. Per an ODASD(IE) report, 45% of power outages at military installations were due to equipment failure. 38% of power outages were due to planned maintenance, 15% from an act of nature and 2% other (Castillo, 2017). The report fails to disclose the context of these power outages. If DoD facilities experience less than .01% downtime a year, how significant is that 45% of that .01%? Regardless, the majority of power outages to DoD facilities reported by the ODASD(IE) were due to equipment failure and very little if any were due to cyber incidents. A reasonable assumption would suggest older facilities and/or equipment need the additional infrastructure for continuity of operations. This in turn gives credence to spend resources on a more robust system rather on defending it.

Per the ODASD website, the ODASD actually oversees the DoD's 880 billion dollar real property portfolio of 28 million acres, 500 military installations with over 562,000 buildings and structures (ODASD, 2017). Understand the dollar amount in real property assets provided by the Defense Manpower Data Center addressed just the Armed Forces. These numbers are larger as it encompasses all of DoD including the other agencies. If the DoD is trying to achieve MA, and in response the ODASD(IE) is to defend through resiliency per 4170.11, where is there concern?

The concern is the dangerous assumption that the threat to DoD real property lies in equipment failure. Without cybersecurity services to perform log monitoring, intrusion detection, or even a honey pot, there is no way of knowing for sure if manipulation of view, control, or safety of control systems affected the loss and denial of view, control, and safety of DoD facility control systems. In short, the DoD cannot say that 45% of power outages were due to equipment failure because there is no evidence to show that the system itself was not compromised.

Finally, any attacks on DoD critical infrastructure that operates within the continental United States and not by another nation-state will need to be apprehended within the confines of the law. Discussed in detail later, Cyber Command operates under Title 10 of the United States Code, and thus falls under the Posse Comitatus Act.

## **4.4 EXTERNAL CHALLENGES**

There are several potential challenges identified that Cyber Command may need to deal with external to the DoD. With the DHS originally tasked with protecting the nation's critical

infrastructure, Cyber Command will need to leverage and work with DHS assets and partners to fully realize their new directives outlined in the 2018 Cyber Strategy. However, in dealing with owners and operators of critical infrastructure, there is evidence to suggest that the DHS has not been as successful as it potentially could be.

#### **4.4.1 Information Sharing:**

In July 2017, the Navy held a Navy-Private Sector Infrastructure Game designed to answer two questions:

1. When do cyber-attacks reach the level of a national security incident?
2. When should the DoD (DOD) be involved and in what capacity?

125 Players from 14 different critical infrastructure sectors across SLTT and federal government. It was determined that private sector companies largely sought to remediate impacts on their own networks without government support, but looked to the DHS and the FBI for information sharing about threats (Schneider, Schechter & Shaffer, 2017). It was determined cyber-attacks against energy, transportation, communications, water/wastewater, and nuclear sectors were declared as a national security incident (Schneider, Schechter & Shaffer, 2017). Again, transportation, communications, water/wastewater are barely covered in current DoD regulations.

#### **4.4.2 Implementation of OT Security:**

LTC Nikki L. Griffin Olive conducted a study with the United States Army War College and came to the conclusion that the DHS has cultivated strong relationships with owners and operations of critical infrastructure, but achieved relatively little successes in implementation and

enforcement of developed security standards and policy (Griffin, 2013). Interestingly, two years later, a similar research was conducted by David Riedman with the Navy Postgraduate School.

David Riedman's research suggests incongruities in defined definitions has led to a mismanagement of personnel and resources. His study suggests the DHS views its mission to defend critical infrastructure facilities different than what federal policies dictate as critical infrastructure (Riedman, 2015). Federal policies state that critical infrastructures are facilities or assets that when damaged or destroyed would have a national impact on that nation's economic security, health, or safety. The DHS sees its mission in protecting all critical infrastructure (Riedman, 2015). In doing so, DHS is negligent in fulfilling its duties to protect critical infrastructure and mishandling resources and effort. The researcher suggests that DHS needs to relook at what is defined as critical, per federal policy and ensure it meets the criteria (Riedman, 2015).

#### **4.4.3 Information Dissemination:**

Each sovereign state and subdivision has created a critical infrastructure cybersecurity and resiliency program. Mason Bradford with the Naval Post Graduate School conducted an anonymous online program evaluation survey of critical infrastructure professionals across the nation in reference to their perception regarding the state and local government's critical infrastructure cybersecurity program. Mr. Bradford's research finds several incongruities. First, is a lack of funding and a lack of dedicated personnel to conduct critical infrastructure cybersecurity. Second, is that the lack of consistency in cybersecurity critical infrastructure programs among the states (Mason, 2015). The Third incongruity Mr. Bradford also sheds light on the disparity between federal and state, organization and classification, between emergency

management and critical infrastructure protection. At the federal level, emergency management and critical infrastructure protection are seen as two discreet parallel workflows (Mason, 2015). However, at the state and local level, it was found that emergency management and critical infrastructure protection programs blend together. He suggests that states standardize a parallel and discreet workflow of emergency management and critical infrastructure protection. Doing so would help streamline goals of secure and resilient national critical infrastructure (Mason, 2015).

Reviewing Mr. Mason's research, it would appear that there is a communication breakdown between controls and risk mitigation strategy from leadership to the operator of control systems. The DHS has put together NIAC and the GCC. Organizations whose purpose is to align cybersecurity objectives and mitigate some of the concerns presented in this research. More research needs to be conducted to validate if this collaboration between industry leaders is providing the change needed at the lowest level. Additionally, to counter Mr. Mason's second concern, it is important to understand that compliance does not necessarily equal security (Conklin, 2017). At some point, it is recommended that security objectives be tailored to the specific industrial control environment based off of the OT Security Principles in figure 2-2.

Finally, it is important to bring up that this is new territory for the DoD. Previously, the DHS had the lead in defending our critical infrastructure through partnerships and exercises (DHS, 2016). These exercises were primarily used to establish procedural responses to disruptions in services provided by critical infrastructure (Nailor, 2018). Now, the DoD is charged with defending our critical infrastructure in a more active posture. Partnerships will need to be cultivated and federal guidelines may be necessary to mark the point of demarcation of responsibility between government and industry responsibilities.

# CHAPTER 5

## 5.1 ADVANCED PERSISTENT THREAT: THE STUXNET DILEMMA

Around 2005-2006, a nation-state began an offensive cyber campaign designed to infiltrate, pilfer, and sabotage industrial control systems against another sovereign nation (Zetter, 2014). It was one of the largest cyber campaigns ever uncovered and it developed some of the most dangerous malware ever created, the most famous of which is called STUXNET. This was not an attack on traditional IT systems. The end goal was not for financial or political gain, but rather to cripple the offensive capability of another nation. The DoD cannot underestimate the implications and importance of a cyber campaign aimed at OT. While most cybersecurity experts are familiar with IT systems and the consequences attacks on traditional IT infrastructure can have, a lot of security professionals are not as familiar with OT.

Countries including China, Russia, North Korea, Iran, Japan, Israel, the UK, and more all have cyber warfare programs. China began developing its offensive capabilities in the late 1990s (Zetter 2014). At least 29 countries have dedicated intelligence or military units for offensive cyber operations (Lendvay, 2016). The militarization of cyber-space is not a new concept. In fact, an attack on the United States critical infrastructure is not a new idea either. In 2001, hackers appearing to originate from China broke into the California Independent System Operator, or Cal-ISO, through two unprotected servers. Cal-ISO manages industrial control systems that move electricity throughout most of California. Had a successful breach occurred, electrical services for the state would have been in jeopardy (Zetter, 2014). In 2002, United States forces in Afghanistan found that Al-Qa'eda had plans to conduct cyber-attacks on dams, using software that could be used to simulate its failure (Harnden, 2002). What is new is the

United States policy in the nation's defense of its critical infrastructure and the digital arms race among countries that equalizes the landscape of cyberwarfare. Enter The Olympic Games.

The Conficker worm infected more than 6 million machines was only 35 kilobytes in size. Most malware is roughly 5 kilobytes in size (Zetter, 2014). STUXNET was 1.18 megabytes in size. Per Kaspersky Labs, Flame, was 20 megabytes in size, more than 650,000 lines of code and 20 times more complicated than STUXNET (Zetter, 2012). It took Symantic and various other Antivirus firms two years to fully understand STUXNET. Kaspersky Labs estimated it would take 10 years to fully understand Flame (Zetter, 2012). Aptly code-named Olympic Games, "Flame," "Duqu," and "STUXNET" were extremely sophisticated malware in a long and successful five year classified campaign aimed at crippling Iran's covert nuclear weapons program (Nakashima, Miller & Tate 2012).

### **5.1.2 Flame:**

Before STUXNET, before Duqu, there was Flame. Flame was an extremely sophisticated espionage tool composed of about 20 modules that would only install malware modules as necessary (Zetter, 2014). It commanded an incredibly large 80 command and control domains that encrypted all data. Only 1,000 victims were struck by flame, systems infected with Flame resided in Iran, Lebanon, Syria, Sudan, and other counties in the surrounding region, suggesting targets were pre-identified (Zetter, 2012). Used to collect intelligence in preparation for STUXNET, Flame secretly mapped and monitored Iran's computer networks (Nakashima, Miller & Tate 2012). Flame spread via the same vulnerabilities as STUXNET, but did not replicate unless given the command by a command and control server (Zetter, 2012). What is most interesting about Flame, was the "God-mode exploit." Flame had vast computational

resources, and extensive knowledge of the Microsoft ecosystem to create a legitimate signed hash transferred to the attacker's falsified digital certificate (Zetter, 2014). Digital certificates are used to authenticate a programs trustworthiness from legitimate companies. The falsified digital certificate attack was described by cryptology researcher, Marc Stevens, as a brilliant feat of mathematics achieved by world-class cryptographers (Zetter, 2014).

### **5.1.3 Duqu:**

Before there was STUXNET, there was Duqu. It is estimated that Duqu was released as early as August 2007, three years before STUXNET was discovered. Duqu, was a Remote Access Trojan used to steal information related to industrial control systems across an intricate command and control network (Symantec, 2011). Duqu would exploit machines at kernel level by taking advantage of a TrueType font-parsing vulnerability. Microsoft uses TrueType to determine how a character should look on screen (Symantec, 2011). Every new machine Duqu infected, had its own command and control proxy server, segmenting information to ensure no one would get the complete picture if compromised (Zetter, 2014). Using proxy servers provided a level of confidentiality to the attackers, as they are used to redirect traffic to another location while keeping the user anonymous. Attackers were particularly interested in AutoCAD files used for drafting 2D and 3D architectural blueprints and mapping out computer networks and machinery on plant floors (Zetter, 2014). Duqu, designed for espionage, deleted all information about itself after the 30th day of infection to reduce the possibility of compromise. Duqu did not replicate (Symantec, 2011). In the end, only about 36 machines were found with Duqu, predominately in Iran and Sudan (Paganini, 2012). Research into STUXNET and Duqu had several common denominators that link them together. Depending on the version of Duqu used, the drivers used by both malware were compiled on the same date and signed with the

same RealTek digital certificate (Zetter, 2014). Drivers found in both malware used algorithms and keys with shared similarities, and analysis of the log files of some of the victims revealed AutoCAD data related to industrial control systems used in various industries in Iran (Zetter, 2014). Duqu and STUXNET had different objectives but the same end goals, debilitating Iran's covert nuclear weapons program.

#### **5.1.4 STUXNET:**

On June 24th, 2010, a small antivirus company named VirusBlockAda would be the undoing of an extremely successful five-year cyber espionage campaign run by nation-state that created one of the most dangerous malware to date (Zetter, 2014). VirusBlockAda uncovered a malware that would later be known as STUXNET and unwittingly ushered the world into a new digital arms race. It could be likened to the nuclear arms race that began in 1945 when the United States dropped a nuclear bomb on Nagasaki and Hiroshima (History, 2018).

STUXNET was a kernel level rootkit designed to sabotage and exploit vulnerabilities in an industrial control system that enriches U-235 isotopes (Lendvay, 2016). History suggests that STUXNET was the first rootkit designed for an industrial control system (Zetter, 2014). STUXNET was used to prevent Iran from developing nuclear weapons at a covert facility in Natanz, but would ultimately end up infecting over 300,000 systems in over 100 countries (Lendvay, 2016). Where Flame and Duqu were controlled, STUXNET left victims all over the world. Surprisingly, the internet was not used to spread this malware and spread only via Universal Serial Bus (USB) and local network connections (Zetter 2014).

At the time when more than 12 million malware programs were captured a year by Symantec, only twelve or so zero-days would be found among them (Zetter, 2014). A zero-day

refers to a vulnerability or exploitable gap in a computer program known only to an attacker, and unknown to the developer or general public (Lendvay, 2016). STUXNET used five. Five zero-day attacks to gain access, escalate privileges, and spread (Zetter, 2014).

	Vulnerability Exploited
1	Windows keyboard file to gain escalated privileges
2	Windows print-spooler functions to spread between machines sharing a printer
3	Windows .LNK files that spread via USB
4	Windows Server Service RPC Handling
5	Buffer-overflow in the wallpaper of Windows (Zetter, 2014)

Table 5-1 STUXNET Zero-Day Attacks (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017)

STUXNET used up to eight different propagation methods, and would take several steps to ensure proper installation and deployment. After STUXNET took root on the system, it would immediately check the antivirus and modified itself accordingly. If STUXNET could not bypass the antivirus scanner it immediately stopped and shut itself down. STUXNET would then install a driver to infect any other USB connected to its system for the next 21 days before installing its layers upon layers of encrypted dynamic link library and configuration file. A dynamic link library is a repository of commonly used programs by the operating system or other applications (Zetter 2014). The developers of STUXNET had a deep understanding of the OT Systems used in the Natanz facilities.

If the machine did not fit the very specific conditions it needed, then STUXNET would shut itself down. STUXNET was targeting machines with very specific configurations of proprietary control system software that ran on top of Windows Operating system, acting as an intermediary between the Windows Operating System and the Siemens Step 7 software. Specifically the S7-315 and S7-417 of Siemens SIMATIC Step 7 software (Zetter, 2014). All in an effort to bypass a physical gap between the control network and the enterprise network.

Waiting for a programmer with STUXNET on his machine to physically connect to a Siemens PLC. STUXNET would then record legitimate PLC commands for 14 days before mimicking them back to the operators while secretly executing its rogue commands (Zetter, 2014). One such rogue command disabled safety systems generated every 100 milliseconds by altering OB35 code sent by the PLC. OB35 is used to indicate if a turbine is operating outside of tolerable conditions (Zetter, 2014).

STUXNET was an intricately crafted malware, obscuring the way it executed code by using the code, inside another block of code in the process of being executed. Then, take that same code being processed and process it in another block of code being executed (Zetter, 2014). STUXNET would monitor its power consumption and utilization of computational resources. Set up file-sharing servers on client machines and infect backend data-bases to ensure each system was infected with the most up-to-date STUXNET version. Perhaps the most impressive accomplishment of them all was that STUXNET, Flame, and Duqu went undetected for five years.

STUXNET was a surgical attack with very specific goals and objectives. Any attack taken on an actual industrial control system would not need to be so sophisticated or require such skill. An attacker would not need malware as dangerous as STUXNET, just a simple 4 kilobyte virus can have devastating consequences. As stated before, an attack on the nation's critical infrastructure is not a new concept.

### **5.1.5 The Olympic Games:**

The United States must remain vigilant against credible threats agents. Whoever was behind STUXNET, Duqu, and Flame cannot assume that they are the only ones with

sophisticated malware, but they are the first to show their hand. A challenge has been given, and nation-states, terrorists, and hacktivists are sure to rise to the challenge. Since STUXNET, there has been a rise in interest in exploiting critical infrastructure. Vupen, a security firm that sells zero-day exploits to nation-states has seen an increase in requests for critical infrastructure (Zetter, 2014).

In 2012, Telvent, a Canadian industrial automation company specializing in SCADA systems for various energy producing industries, was hacked by attackers linked to the Chinese Military (Krebs, 2012). The Chinese Military stole project files for SCADA systems they produced and managed for their customers. Of note, one project file stolen was for a product for energy firms for smart grid technology to be backwards compatible with legacy assets (Krebs, 2012).

In 2013, Iran had compromised the command-and-control system of the Rye Brook Dam in New York using a cellular modem. The incident was not reported by the United States until 2016, but speculation was it could have been a test run for a larger dam in the United States (Berger, 2016). Ransomware is even making its way into OT systems as well. As early as 2013, ransomware hit a mining company's industrial control network. The operator paid over 100 thousand dollars to regain access to the HMIs (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). Per the Washington Post, North Korea was apparently behind the infamous WannaCry ransomware attack that affected over 230,000 computers in over 150 countries in early 2017 (Nakashima & Rucker, 2017). It would not be a hard sell to see North Korean attackers pivot into industrial control systems.

According to IBM's Managed Security Services Data, attacks on industrial control systems rose 110% from 2015 to 2016. 60% of those attacks were against the United States critical infrastructure (McMillen, 2016).

China's Telvent Hack was an attempt to gather data on SCADA systems used in critical infrastructure around the world. Nation-states have plans and counter-plans just as the United States. A lot of effort went into sabotaging another nation's critical infrastructure. How much further would they be willing to go if it was the United States?

Will there be further ramifications and retaliation when Iran and North Korea acquire offensive cyber capabilities seen by STUXNET, Duqu, and Flame? As with STUXNET, Flame, and Duqu, no one has claimed ownership, and proving attribution in cyber can be difficult. To prove attribution, a forensic analysis of static and live data is helpful to ascertain the "who, what, when, why, and how." Should industry decide to take legal action, any evidence gleaned from a forensics analysis needs to be handled appropriately to be used as evidence in the court of law (Ahmed, Naedele, Obermeier, & Richard, 2012). The intricacy of forensic analysis is a separate topic, but it is still an important issue that would be remiss if not brought to light. As SCADA forensics is still a relatively new field, with few if any guidelines available (Ahmed, Naedele, Obermeier, & Richard, 2012).

Academia has proposed some frameworks. Researchers attending the 2013 Industrial Control System and Cyber Security Research proceedings detailed a proposed method using IT forensic techniques on SCADA servers (Wu, Pagna Disso, Jones & Campos, 2013). Lewis Folkerth with the SANS Technology Institute was able to develop some techniques for forensic analysis that was tested on a live ICS that resulted in successful recovery and detection after the

incident, but not attribution (Folkerth, 2015). If Cyber Command fails to defend the nation's critical infrastructure, how will attribution be determined? How attribution will impact Combatant Commanders' potential effect on the operational environment needs to be clarified.

# CHAPTER 6

## 6.1 THE WAY FORWARD

### 6.1.1 Critical Infrastructure Protection Teams:

Industrial control system Cybersecurity professionals require a set of unique skills beyond networking hardware and operating systems commonly found in most enterprise businesses. It is a multidiscipline understanding of control systems coupled with physics and engineering requirements of industrial control processes (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

### 6.1.2 Training:

While the opinions of this author are that Cyber Command should not defend OT networks and systems outlined in Zones 0-3, there are some tools commonly found in IT networks are also useful in OT networks, while others are OT specific. Just as the Army has Soldiers with specialized designated skill sets, so too must the industrial control system cybersecurity professional. Categorized and listed below are common control system tools that can assist the next generation of industrial control system security professionals. This is not a comprehensive list, but rather some suggestions on skill sets that could be cultivated depending on the level of partnership agreement the Cyber Command has with the owner or operators of the control system.

**Network Monitoring:** Devices in OT networks communicate in a pre-defined manner. Data flow is predetermined and identification and monitoring of proper data across the OT network is possible with programs like Snort, Suricata, and the Brother Network Security Monitor (Conklin, 2017).

**Asset Identification:** WireShark, Grassmarlin, or Sophia. Grassmarlin is a free NSA tool used by industrial control system networks to identify devices on the network and extract the data they contain (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**Vulnerability Assessment:** Several open source, online tools, can be utilized to determine what OT device has what vulnerability. Examples include the National Vulnerability Database, Common Exposures Database and ICS-CERT advisories (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). A great tool provided for free by DHS is The Cyber Security Evaluation Tool or CSET that provides a comprehensive vulnerability overview of industry specific industrial control systems (ICS-CERT, 2016). Asks questions about policy, risk, stakeholders, and detailed questions as it pertains to the sector operated in.

**Configuration Review:** OT security professionals will need a control system baseline with hardware configurations, copies of current ladder logic programs and a list of all devices attached to the OT network (Folkerth, 2015). There are several automated tools that assist with ensuring that common devices found in the industrial control system are as a secure as possible. Examples include Nipper and Nessus (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

**Penetration Testing (Pentesting):** Penetration testing is used in conjunction with a risk assessment, to validate the current cybersecurity posture, or verify security controls are operating as intended (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017). When conducting penetration testing in an OT environment, it should be virtualized. If, on the rare occasion that the control system has a lab or a mini replicated system for research and development that can simulate the real-world control system, then use if available. Some tools, Shodan.io, Kali Linux, Scans.io, Censys.io (Conklin, 2017). If this cannot be done, and leadership still wants a pentest done to complete a valid risk assessment, then clear rules of engagement must be developed, understood and risk accepted by a designated approving authority (Bodungen, Singer, Shbeeb, Hilt & Wilhoit, 2017).

Tools outlined above are useless unless control system security professionals know what they are looking for. Wireshark, a useful tool for packet analysis and asset identification, is a free tool that can assist critical infrastructure protection teams in performing deep packet analysis. Packets that may contain protocols for OT systems where there should not be. If the DMZ is configured appropriately, there should not be protocols used in control systems outside of Zones 0-3. Protocols in zones 0-3 will all be predefined so anomalies tend to stick out.

Logging is another action that should be taken by control system security professionals to log events and protocols.

Control system security professionals will need to have a plan to handle incidents and responses to OT networks. A dedicated team with specialized skill sets outlined earlier will need to be trained and need to work together. A perfect resource is The Idaho National Lab. They have a full-scale electric power grid that is dedicated to controlling system cybersecurity assessment, standards improvements, and training (Ahmed, Naedele, Obermeier, & Richard, 2012).

## 6.2 SUSTAINS

The DoD is not without support in its new-found mission to defend the United States' critical infrastructure. The Armed Forces, DHS, Cyber Command, pre-established partnerships with industry stakeholders, ODASD(IE), NIST, policy, financial support, and others. Cyber Command has a slew of support both internal to the DoD and external, that it needs to leverage if Cyber Command is to be successful in defending the nation's critical infrastructure. The challenge will be to consolidate, organize, and restructure as appropriate. Support available to Cyber Command is outlined below.

### 6.2.1 Policy and Funds:

Policies such as the DoDI 4170.11, 3020.45 and DoD Directive 30.20.40 are all directives that had some great frameworks and tools that can still be leveraged. The National Defense Authorization Act (NDAA) for Fiscal Year 2017 provides funding for the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of the critical infrastructure of the

DoD (NDAA, 2017). Surprisingly, there is also funding to prevent Electromagnetic Interference (EMI) and radio frequency weapons (RFWs) to our critical infrastructure (NDAA, 2017). The use of RFWs is an entirely separate topic, however it should be noted that RFWs can potentially be used to affect, remote terminal units, actuators, and other systems that use wireless for communication to have unintentional consequences, valve closures, disabled communications, false data transmissions, and damage to the electronic device itself to name a few (TSWG, 2005). It is interesting to note that per the 2017 NDAA the United States authorizes funds to address the need to answer Russia's doctrine with respect to targeting adversary critical infrastructure (NDAA, 2017).

National Defense Authorization Act for Fiscal Year 2018 provides funding for assistance via the Armed Forces, DoD civilians employees and subject matter experts in industry and government to assist the DoD in the cybersecurity of critical infrastructure. The 2018 NDAA also stipulates that they are to conduct appropriate cybersecurity review of existing systems and infrastructure as well as acquisition plans for proposed systems and infrastructure.

### **6.2.2 Armed Forces:**

Cyber Command's Air Forces Cyber and the Navy has already made some headway into OT. However, the National Guard is a potential asset Cyber Command could leverage. Christopher Baker thought of using the National Guard as an option available to DoD in enabling the transition of shared information and collaboration in defending critical infrastructure. In a rare case, the Michigan National Guard is at the forefront in industrial control system cybersecurity. The Michigan National Guard built a cybersecurity range to meet the cybersecurity needs of prevention, protection, mitigation, and response to cyber incidents (Baker, 2015). The Michigan Public Service Commission even collaborates with critical infrastructure

owners and operators to protect energy control systems from cyber-attacks that could jeopardize public health and safety (Baker, 2015). As the Guard falls under Title 32 and not Title 10, it could operate in some form of state authority. It would require some coordination between federal entities and various state Title 32 leadership to conform to a streamlined alignment of National Guard CIP capabilities across the states (Baker, 2015).

Another benefit the DoD has with National Guard partnership, is that the National Guard does not fall under the Posse Comitatus Act, which enables the National Guard to perform police functions. Theoretically, the National Guard could not only “defend OT networks, but search for and apprehend offenders that infiltrate CIKR networks” (Baker, 2015). This could give the DoD the ability to legally respond to incidents inside the continental United States and legitimize the 2018 Cyber Strategy’s defensive posture internal to the United States. What is key to differentiate is that with the National Guard, the potential of having civilian critical infrastructure owners and operators as subject matter experts in the fight is invaluable. With the limited experience DoD has in this field, leveraging National Guard Assets like in Michigan could prove fruitful.

Of note, this does not absolve critical infrastructure owners and operators of the responsibility to safeguard their OT systems, but rather enables their critical infrastructure protection teams to have additional help and resources in defending their OT networks.

In the same manner of collaboration with the National Guard, the DoD could leverage the Federal Reserve Forces. Doing so would enable warrior citizens working in the local community to cross-pollinate industry standards and cybersecurity best practices to the DoD critical infrastructure.

### **6.2.3 Partnerships:**

Cyber Command should continue to cultivate the relationships built by DHS with industry to better enhance collaboration. These relationships have led to several OT cyber exercises that have better postured the United States to defend and respond to cyber-attacks against industrial control systems. A great example of leveraging partnerships with industry and the United States government is the DoD's Cyber Guard. Perhaps the largest annual critical infrastructure exercise conducted by the DoD includes Cyber Command, DHS, and the FBI. The DoD conducts an annual exercise program with DHS and the FBI for contingencies against cyber threats to the nation's critical infrastructure on a massive scale. Purpose is to have a "whole-of-nation response" to a massive cyberattack to the United States critical infrastructure (Cyber Guard, 2016). The exercise provides innovative approaches to defending United States critical infrastructure, integration of industry and federal support, training, and situational understanding (Cyber Guard, 2016).

The NCCIC's Cyber Storm is another great example of collaboration with industry. The NCCIC's primary function is to promote shared situational awareness of malicious cyber activity against the United States critical infrastructure and key resources (Zetter, 2014). One of the ways the NCCIC does this is through a digital exercise called Cyber Storm. A biennial exercise to answer the critical question: "How would government agencies and critical infrastructure owners and operators respond to an attack against national critical infrastructure?" (NCCIC, 2018) The exercise involved more than 1,000 participants (or "players") around the globe, from various federal, state, and local law enforcement authorities. This exercise was executed online to allow players to participate from their work location. The exercise is not technical, but more operational focused, working out the process and procedures for proper collaboration of

information and responses (Nailor, 2018). The federal government's partnership with industry has been beneficial in getting support from key leaders in enhancing the cybersecurity of OT systems.

Cyber Command also has the benefit of the DHS establishing support within the Government to defend the nation's critical infrastructure. The FBI provides a domestic legal sanction to prosecute attacks committed by individuals that reside within the continental United States (FBI, n.d.). The FBI's Cyber Division, the DSAC and InfraGard program are perfect assets to compliment Cyber Commands ability to protect the nations critical infrastructure in a legal and authorized manner.

As Cyber Command continues to gain operational understanding of the threat environment affecting OT systems, a symbiotic relationship should be cultivated with the Department of Commerce's NIST. As threats to OT infrastructure are better understood, Cyber Command and NIST can enhance the quality and maintain the relevance of special publications for threats, vulnerabilities, and countermeasures in SCADA and DCS infrastructures. These special publications released by NIST has some recommendations for OT in facilities and buildings such as fire alarms, lights, physical access control, building management control systems and more (Stouffer, Lightman, Abrams & Hahn, 2015). A partnership between NIST, the ODASD(IE) and Cyber Command could help strengthen the ODASD(IE)'s policy, strategy, and cybersecurity of DoD facility related control systems.

While critical infrastructure plays a strategic role in our nation's security, the United States must focus on key resources and key points of interest to have any kind of effective security. The DHS and the DoD cannot defend every network and system that operates under its

purview. The attack surface is too large to defend against all threats and too vast to close all vulnerabilities (Hackney, n.d.). The United States must identify, prioritize, and defend its most important assets (Riedman, 2015). However, the United States cannot let other vulnerabilities go by the way side either. A careful balance must be struck while empowering others through shared knowledge and assistance to defend its OT systems must become a priority.

# CHAPTER 7

## 7.1 CONCLUSION

The DoD operates predominately in the IT domain, not in OT. Historically speaking, the DoD has little involvement in securing OT used in critical infrastructure. In the 2018 Cyber Security Strategy, the cybersecurity of the nation's critical infrastructure has evolved from a passive defense through collaborative partnership with industry owners and operators to a more aggressive "defend forward" posture. However, the DoD has yet to address who in the DoD will assume the mission to defend the nations critical infrastructure, and how it will be accomplished. This research addressed these questions and the reasons leading up to the DoD's sudden change in policy. The findings of this research is as follows:

1. Cyber Command is best positioned to assume the mission to defend the nation's critical infrastructure.
2. Cyber Command will need to address several internal challenges before moving forward. Key challenges:
  - a. DoD regulations and policies concerning the cybersecurity of OT must be updated.
  - b. Updated OT cybersecurity regulations and policies must standardize and enforce baseline OT security requirements across the DoD.
  - c. Updates and additions to DCI capability must first ensure that baseline cybersecurity requirements are met.
3. Cyber Command will need to have a dedicated OT specialized protection teams with the following support:
  - a. Trained OT security professionals with a basic understanding of the OT environment and the associated skillset needed to defend a network they cannot touch.

- b. Clearly defined boundaries and rules of engagement. Depending on Cyber Command's aggressiveness in its role to defend DCI, recommendations are to operate only in level 4 and 5 of the Purdue Model.
- c. Partnerships with DHS, FBI, NIST, FERC, SLTT and industry must continue to work together for collaboration and training exercises.

Cyber Command will need to deal with external challenges of managing the protection of the nation's critical infrastructure. Advanced persistent threats, originating from nation-states, are developing cutting-edge malware aimed at exploiting vulnerabilities in critical infrastructure and key resources. With the advent of STUXNET, a new digital arms race has been launched, but the manner in which this arms race is conducted has yet to be truly understood or seen. Nation-states are stealing information related to control systems and security firms are being solicited to find vulnerabilities in OT for future exploitation. Even ransomware is beginning to emerge in OT. As General Oderieno once stated, we are indeed entering a more complex future environment.

However, the United States Government has the infrastructure and systems in place to affect change from the top down. Industry and government best practices like the Purdue Model, Top 20 for ICS, and Special Publications provide a good foundation to apply OT cybersecurity based off AIC security principles. The DHS has established partnerships in both government and industry that can be leveraged by Cyber Command. Whatever actions conducted by the DoD to defend the nation's critical infrastructure, must be done within the confines of the law. Should an attack on our critical infrastructure occur within the nation's borders, Cyber Command could leverage the FBI or possibly the National Guard for prosecution. Appropriate responses to threat agents located OCONUS attacking, sabotaging, or conducting espionage to the nation's critical infrastructure should be clearly defined in the rules of engagement.

Whatever the future holds, the United States leadership needs to understand the ramifications of any actions taken under the 2018 Cyber Defense Strategy will have repercussions. That when it comes to critical infrastructure, the United States has the most to lose.

# GLOSSARY OF ABBREVIATIONS:

AFCEC-AFCYBER – Air Force Civil Engineer Center-Air Force Cyber Nexus Collaboration

AIC – Availability, Integrity, Confidentiality

CIA – Confidentiality, Integrity, and Availability

CIKR – Critical Infrastructure and Key Resources

CIP - Critical Infrastructure Protection

CONUS – The Continental United States

CRC – Cyclic Redundancy Checks

DCI – Defense Critical Infrastructure

DCIP – DoD Protected Critical Infrastructure Program

DCS – Distributed Control System

DHS – Department of Homeland Security

DIB – Defense Industrial Base

DISA – Defense Information Systems Agency

DLA – Defense Logistics Agency

DMZ – Demilitarized Zone

DNP3.0 – Distributed Network Protocol

DoD – Department of Defense

DoDI – Department of Defense Instruction

DOE – Department of Energy

DON – Department of the Navy

DON CIP – Department of the Navy Critical Infrastructure Program

DSAC – Domestic Security Alliance Council

EUC – Equipment Under Control

FBI – Federal Bureau of Investigation

FERC – Federal Energy Regulatory Commission

FERC – Federal Energy Regulatory Commission

GCC – Government Coordinating Council

GSA - General Services Administration

HMI – Human Machine Interface

HSPD – Homeland Security Presidential Directive

ICCP – Inter Control Center Protocol

IEC – International Electrotechnical Commission

IT – Information Technology

MA – Mission Assurance

NCCIC – National Cybersecurity and Communications Integration Center

NDAA – National Defense Authorization Act

NIAC – National Infrastructure Advisory Committee

NIPP – National Infrastructure Plan

NIST – National Institute of Standards and Technology

NSA – National Security Agency

OCONUS – Outside the Continental United States

ODASD – The Office of the Assistant Secretary of Defense for Energy, Installations, and Environment

ODASD(IE) – The Office of the Assistant Secretary of Defense for Energy, Installations, and Environment Installation Energy

OT – Operational Technology

PDD – Presidential Decision Directive

PDU – Protocol Data Units

PLC – Programmable Logic Controller

RFW – Radio Frequency Weapons

RTU – Remote Terminal Units

SCADA – Supervisory Control and Data Acquisition

SIS – Safety Instrumented Systems

SLTT – State, local, tribal, and territorial

TCP – Transmission Control Protocol

UCP – Unified Command Plan

UDP – User Datagram Protocol

USB – Universal Serial Bus

VFD – Variable Frequency Drive

## REFERENCES

- AFCEC. (n.d). *Air Force Civil Engineer Center: What We Do: Energy*. Retrieved from: <https://www.afcec.af.mil/Home/Energy/>
- Aggerwal S. (2014). Greasing the Electric Grid, the World's Largest Machine (Op-Ed). Retrieved from: <https://www.livescience.com/48893-improving-efficiency-on-the-electric-grid.html>
- Ahmed, I., Naedele, M., Obermeier, S., & Richard, G.G. (2012) *SCADA Systems: Challenges for Forensic Investigators*. Retrieved from: <https://ieeexplore.ieee.org/document/6298895>
- Ausley, A. (2014). *AFCEC, AFCYBER partnership boosts infrastructure security*. Retrieved from <https://www.af.mil/news/article-display/article/485520/afcec-afcyber-partnership-boosts-infrastructure-security/>
- Baker, C. J. (2015). *Cybersecurity for Critical Infrastructure*. Retrieved from: [www.dtic.mil/dtic/tr/fulltext/u2/1012791.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/1012791.pdf)
- Berger, J. (2016). *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*. Retrieved from: <https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html>
- Bodungen, C. E., Singer, B. L., Shbeeb, A., Hilt, S., & Wilhoit K. (2017). *Hacking Industrial Control Systems Exposed: ICS and SCADA Security Secrets and Solutions*. McGraw- Hill
- Byres, E. (n.d.). *Unicorns and Air Gaps – Do They Really Exist? Living with Reality in Critical Infrastructures*. Tofino.
- Carter, R. (2017). *Protecting critical infrastructure from cyber threats information technology systems*. Retrieved from: <http://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1324406/protecting-critical-infrastructure-from-cyber-threats-information-technology-sy/>
- Castillo, Ariel. (2017). *Department of Defense Installation Energy: OSD Energy Resilience Overview Energy Planning for Resilient Military Installations*. Retrieved from: <https://www.acq.osd.mil/eie/downloads/2017>
- CIS. (2018). *Center for Internet Security Controls*. Retrieved from: <https://www.cisecurity.org/>
- CNN. (2008). *Probe: Engineer's actions triggered Florida blackout*. Retrieved <http://www.cnn.com/2008/US/02/29/florida.outage/index.html>
- Conklin, W. A. (2016). *Introduction to Control Systems*. Texas.

- Conklin, W. A. (2016). *Security Controls for Industrial Control Systems*. Texas.
- Conklin, W. A. (2017). *Controls System Networks*. Texas.
- Conklin, W. A. (2018). *ICS Threat Space*. Texas.
- Conklin, W. A. (2018). *Security Controls for Industrial Control System*. Texas
- Cornel Law School. (n.d.). *10 U.S. Code § 191 - Secretary of Defense: authority to provide for common performance of supply or service activities*. Retrieved from: <https://www.law.cornell.edu/uscode/text/10/191>
- Cornel Law School. (n.d.). *10 U.S. Code § 193 - Combat support agencies: oversight*. Retrieved from: <https://www.law.cornell.edu/uscode/text/10/193>
- Covey, S. (1989). *The 7 Habits of Highly Effective People*. Free Press.
- Cyber Guard. (2016). *U.S. Cyber Command Cyber Guard 16 Fact Sheet*. Retrieved from: <https://dod.defense.gov/Portals/1/...cyber.../Cyber-Guard-16-FactSheet-FINAL.pdf>
- CYBERCOM. (2018). *U.S. Cyber Command History*. Retrieved from: <https://www.cybercom.mil/About/History/>
- DHS. (2001). *National Infrastructure Advisory Council Authorities: Executive Order 13231 of October 16, 2001 (Continuance of the NIAC)*. Retrieved from: <https://www.dhs.gov/publication/niac-authorities>
- DHS. (2002). *Protected Critical Infrastructure Information (PCII) Program. (Continuance of the NIAC)*. Retrieved from <https://www.dhs.gov/pcii-program>
- DHS. (2009). *Critical Infrastructure Resilience: Final Report and Recommendations*. Retrieved from: <https://www.dhs.gov/publication/niac-critical-infrastructure-resilience-final-report>
- DHS. (2009). *National Infrastructure Protection Plan 2009: Partnering to Enhance Protection and Resiliency*. Retrieved from: <https://www.dhs.gov/publication//nipp-2009-partnering-enhance-protection-resiliency>
- DHS. (2013). *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resiliency*. Retrieved from: <https://www.dhs.gov/publication//nipp-2009-partnering-for-critical-infrastructure-security-and-resiliency>

- DHS. (2015). *Government Facilities Sector-Specific Plan: An annex to the NIPP 2013*. Retrieved from: <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf>
- DHS. (2015). *Homeland Security Presidential Directive 7*. Retrieved from: <https://www.dhs.gov/homeland-security-presidential-directive-7>
- DHS. (2016). *Prevent Terrorism and Enhance Security*. Retrieved from: <https://www.dhs.gov/prevent-terrorism-and-enhance-security>
- DHS. (2018). *Department of Homeland Security: Critical Infrastructure Sector Partnerships*. Retrieved from: <https://www.dhs.gov/critical-infrastructure-sector-partnerships>
- DHS. (2018). *Department of Homeland Security: Using the Cybersecurity Framework*. Retrieved from: <https://www.dhs.gov/using-cybersecurity-framework>
- DISA. (n.d.). *Defense Information Systems Agency: About DISA*. Retrieved from: <https://www.disa.mil/About>
- DISA. (n.d.). *DISA: Network Services*. Retrieved from: <https://www.disa.mil/network-services>
- DLA RFP. (2018). *Utilities Privatization RFP Schedule Air Force/Army*. Retrieved from: <https://www.google.com/search?q=Utilities%20Privatization%20RFP%20Schedule&cad=h#>
- DLA. (n.d.). *DLA Energy: History of DLA Energy*. Retrieved from: <http://www.dla.mil/energy/about/history.aspx>
- DLA. (n.d.). *DLA Energy: Utility Services*. Retrieved from: <http://www.dla.mil/energy/offers/services/utilityservices.aspx>
- DLA. (n.d.). *History of DLA Energy*. Retrieved from <http://www.dla.mil/Energy/About/History/>
- DMDC. (2017). *The Defense Manpower Data Center (DMDC): Base Structure Report – Fiscal Year 2017 Baseline*. <https://www.acq.osd.mil/eie/Downloads/BSI/Base%20Structure%20Report%20FY17.pdf>
- DNP. (2012). *A Forum for Supporters of the Distributed Network Protocol*. Retrieved from: <https://www.dnp.org/default.aspx>
- DoD Cyber Strategy. (2015). *The DoD Cyber Strategy*. Retrieved from: [http://archive.defense.gov/home/features/2015/0415\\_cyber-strategy/](http://archive.defense.gov/home/features/2015/0415_cyber-strategy/)
- DoD Cyber Strategy. (2018). *Summary DoD Cyber Strategy*. Retrieved from: [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber\\_strategy\\_summary\\_final.pdf](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf)

- DoD SSPP. (2016). *Department of Defense Strategic Sustainability Performance Plan FY 2016*. Retrieved from: <https://www.denix.osd.mil/sustainability/dod-sspp/unassigned/department-of-defense-strategic-sustainability-performance-plan-fy-2016/>
- DoD. (2000). *Department of Defense Guidance for Privatizing Defense Utility Systems*. Retrieved from: <https://www.acq.osd.mil/eie/Downloads/IE/guidance.pdf>
- DoD. (n.d.). *Our Story*. Retrieved from: <https://www.defense.gov/Our-Story/>
- DoDD 3020.40. (2016). *Department of Defense Directive: Mission Assurance (MA)*. Retrieved From: [www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf)
- DoDI 3020.45. (2018). *Department of Defense Instruction: Mission Assurance (MA) Construct*. Retrieved from: <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=2018-08-14-081232-450>
- DoDI 4170.11. (2016). *Office of the Assistant Secretary of Defense for Energy, Installations, and Environment Installation Energy: Installation Energy Policy and Program Guidance*. Retrieved from the ODASD (IE): [https://www.acq.osd.mil/eie/IE/FEP\\_Policy\\_Program\\_Guidance.html](https://www.acq.osd.mil/eie/IE/FEP_Policy_Program_Guidance.html)
- DoDM 3020.45. (2017). *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*. Retrieved from: <https://www.hsdl.org/?abstract&did=801336>
- DOE. (2012). *2010 Smart Grid System Report: Report to Congress*. Retrieved from: <https://www.energy.gov/sites/prod/files/2010%20Smart%20Grid%20System%20Report.pdf>
- DOE. (2014). *U.S. Department of Energy: Federal Building Metering Guidance*. Retrieved from: [https://www.energy.gov/sites/prod/files/2014/11/f19/metering\\_guidance.pdf](https://www.energy.gov/sites/prod/files/2014/11/f19/metering_guidance.pdf)
- DON CIP. (2009). *Department of the Navy Critical Infrastructure Protection Program Strategy for 2009 and Beyond*. Retrieved from: [www.doncio.navy.mil/uploads/1019VYV97598.pdf](http://www.doncio.navy.mil/uploads/1019VYV97598.pdf)
- DSAC. (n.d.). *Domestic Security Alliance Council: About DSAC*. Retrieved from: <https://www.dsac.gov/about>
- FBI. (n.d.). *Addressing Threats to the Nation's Cybersecurity*. Retrieved from: <https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view>

- FERC. (2018). *Federal Energy Regulatory Commission: Cyber & Grid Security*. Retrieved from: <https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp>
- FERC. (2018). *Federal Energy Regulatory Commission: What FERC Does*. Retrieved from: <https://www.ferc.gov/about/ferc-does.asp?csrt=6287279062985997223>
- FM 3-0. (2017). *Field Manual 3-0: Operations*. Retrieved From: [https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB\\_ID=1003121](https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1003121)
- FM 6-0. (2014). *Field Manual 6-0: Commander and Staff Organization and Operations*. Retrieved from: <https://armypubs.army.mil/ProductMaps/PubForm/FM.aspx>
- Folkerth, L. (2015). *Forensic Analysis of Industrial Control Systems*. Retrieved from: <https://www.sans.org/reading-room/whitepapers/forensics/paper/36277>
- Gartner. (n.d). *Operational Technology*. Retrieved from: <https://www.gartner.com/it-glossary/operational-technology-ot/>
- Google. (n.d.). *Information Technology*. Retrieved from: <https://www.google.com/search?q=information%20technology%20definition&cad=h>
- Greenplant. (2011). *Distributed Control System or DCS: Brief History*. Retrieved from: <http://whatisinstrumentation.blogspot.com/2012/12/distributed-control-system-or-dcs-brief.html>
- GSA. (2014). *Improving Cybersecurity and Resilience through Acquisition*. Retrieved from <https://www.gsa.gov/policy-regulations/policy/information-integrity-and-access/cybersecurity-policy>
- Hackney, C. (n.d.). *The Next Generation of Defensive Cyberspace Operations*. Retrieved from: <https://www.uscybersecurity.net/cybersecuritychannel/csios-corporation/>
- Harnden, T. (2002). *Al-Qa'eda Plans Cyber Attacks On Dams*. Retrieved from <https://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qaeda-plans-cyber-attacks-on-dams.html>
- Harris, S. (2013). *CISSP All-in-One Exam Guide*. McGraw- Hill
- History. (2018). *Bombing of Hiroshima and Nagasaki*. Retrieved from: <https://www.history.com/topics/world-war-ii/bombing-of-hiroshima-and-nagasaki>
- ICS-CERT. (2016). *Industrial Control System Cyber Emergency Response Team: Assessment Program Overview*. Retrieved from: <https://ics-cert.us-cert.gov/Assessments>
- IEC 61508. (n.d.). *Functional Safety and IEC 61508*: Retrieved from: <http://www.iec.ch/functionalsafety/>

- InfraGard. (n.d.). *Welcome to Infragard*. Retrieved from: <https://www.infragard.org/Application/Account/Login>
- JP 3-0. (n.d.). *Joint Publication: Joint Operations*. Retrieved from: <http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>
- Knapp, E.D., Langili, J. (2014). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress.
- Krebs, B. (2012). *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*. Retrieved from: <https://krebsonsecurity.com/tag/telvent-hack/>
- Krebs, B. (2014). *Target Hackers Broke in Via HVAC Company*. Retrieved from: <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>
- Lendvay, R. L. (2016). *Shadows of STUXNET: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived From the STUXNET Attack*. Retrieved from: <https://www.hsdl.org/?view&did=792239>
- Luciano, C. (2018). *Hybrid renewable energy project wins Secretary of the Army Award*. Retrieved from: [http://www.forthoodsentinel.com/news/hybrid-renewable-energy-project-wins-secretary-of-the-army-award/article\\_87c61b96-ab97-11e8-9c7c-bbdd46e763f4.html](http://www.forthoodsentinel.com/news/hybrid-renewable-energy-project-wins-secretary-of-the-army-award/article_87c61b96-ab97-11e8-9c7c-bbdd46e763f4.html)
- Martin, C. (2006). *Protecting America's Critical Infrastructure: Making Our Program More*. Retrieved from: [www.dtic.mil/dtic/tr/fulltext/u2/a448435.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/a448435.pdf)
- Mason, B.C. (2015). *Putting the Critical Back in Critical Infrastructure*. Retrieved from: [www.dtic.mil/dtic/tr/fulltext/u2/1009160.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/1009160.pdf)
- McMillen, D. (2016). *Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent*. Retrieved from: <https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/>
- Mitchell, E. (2018). *Policy issues take center stage as House panel passes \$716B defense authorization bill*. Retrieved from: <https://thehill.com/policy/defense/387050-policy-issues-take-center-stage-as-house-panel-passes-716b-defense>
- ModBus. (2018). *Modbus FAQ: About the Protocol*. Retrieved from: <http://www.modbus.org/faq.php>
- Nakashima, E. Miller, G., Tate, J. (2012). *U.S., Israel, Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*. Retrieved from: <https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian->

nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV\_story.html?utm\_term=.fc23f19ea344

Nakashima, E., Rucker, P. (2017). *U.S. Declares North Korea carried out massive WannaCry cyberattack*. Retrieved from: [https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e\\_story.html?utm\\_term=.074ce1c590bf](https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?utm_term=.074ce1c590bf)

Naylor, B. (2018). *3 Days Of War Games Test Government Response To Serious Cyberattacks*. Retrieved from: <https://www.npr.org/2018/04/12/601217231/cyber-storm-tests-government-reaction-to-cyberattacks-amid-increasing-threats>

NCCIC. (2018). *Cyber Storm IV: National Cyber Exercise*. Retrieved from: <https://www.dhs.gov/cyber-storm-vi>

NDAA. (2017). National Defense Authorization Act for Fiscal Year 2017. Retrieved from: <https://www.congress.gov/bill/114th-congress/senate-bill/2943/text>

NDAA. (2018). National Defense Authorization Act for Fiscal Year 2018. Retrieved from: <https://www.congress.gov/bill/115th-congress/house-bill/2810>

NERC. (2006). *FERC Order 18 CRF Part 39- Rules Concerning Cert of ERO*. Retrieved from: <https://www.nerc.com/pa/Stand/Resources/Pages/Default.aspx>

NERC. (2012). History of NERC. Retrieved from: [https://www.nerc.com/AboutNERC/Documents/History\\_Dec12.pdf](https://www.nerc.com/AboutNERC/Documents/History_Dec12.pdf)

NERC. (n.d). *Mandatory Standards Subject to Enforcement*. Retrieved from: <https://www.nerc.net/standardsreports/standardssummary.aspx>

NSA. (n.d.). NSA CSS: Frequently Asked Questions about Signals Intelligence (SIGINT). Retrieved from: <https://www.nsa.gov/about/faqs/sigint-faqs/>

NSA. (n.d.). *NSA CSS: Mission and Values*. Retrieved from: <https://www.nsa.gov/about/mission-values/>

ODASD(IE). (2002). *DoD Guidance For Privatizing Defense Utility Systems*. Retrieved from: <https://www.acq.osd.mil/eie/Downloads/IE/guidance.pdf>

ODASD(IE). (n.d.). *Office of the Assistant Secretary of Defense for Energy, Installations, and Environment Installation Energy (ODASD(IE)): Installation Energy*. Retrieved from the ODASD (IE): [https://www.acq.osd.mil/eie/IE/FEP\\_index.html](https://www.acq.osd.mil/eie/IE/FEP_index.html)

- ODASD. (2007). *Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (ODASD): Leadership*. Retrieved from the ODASD: <https://www.acq.osd.mil/eie/Bios.html>
- Odierno, R. (2012, August 24). *World Affairs: US Army Chief of Staff Gen Raymond T. Odierno on America's Army: The Strength of the Nation*. Retrieved from: [www.worldaffairs.org/speakers/profile/raymond-odierno.html](http://www.worldaffairs.org/speakers/profile/raymond-odierno.html)
- Olive, N., L., G. (2013). *Cybersecurity: The Nation's Greatest Threat To Critical Infrastructure*. Retrieved from: [www.dtic.mil/dtic/tr/fulltext/u2/a589328.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/a589328.pdf)
- Paganini P. (2012). *Security Affairs: Duqu – Cyber Weapons Factory Still Operating... It's Just The Begging*. Retrieved from: <https://securityaffairs.co/wordpress/3716/malware/duqu-cyber-weapons-factory-still-operating-its-just-the-beginning.html>
- Pawar, R., Bhasme, N. R. (2016). *Application of PLC's for Automation of Processes in Industries*. Journal of Engineering Research and Applications. Vol. 6, Issue 6, pp. 53-59.
- PPD-63, (1998). 63 FR 41804 – Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators. Retrieved from: <https://www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865>
- Reiter, D. (2005). *DON CIP: A Comprehensive Solution to Improve Cyber and Physical Security of DON Critical Assets*. Retrieved from: <http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3232>
- Riedman, D.A. (2015). *How Critical is Critical Infrastructure?* Retrieved from: <https://www.hsaj.org/articles/8092>
- Rotimi, K. (2018). *NSA CSS: In the Spotlight: Kolade "Yemi" Rotimi*. Retrieved from: <https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1654921/in-the-spotlight-kolade-yemi-rotimi/>
- Schneider, J., Schechter, B., Shaffer, R. (2017). *Navy-Private Sector Critical Infrastructure War Game 2017 Game Report*. Retrieved from: <http://www.nwcfoundation.org/Files/Admin/Corp%20Logos/Navy-rivate%20Sector%20Critical%20Infrastructure%20War%20Game%20Report%20%281%29%20%282%29.pdf>
- Stouffer, K., Lightman, V.P., Abrams, M., Hahn, A. (2015). *NIST Special Publication 800-82r2: Guide to Industrial Control Systems (ICS) Security*. Retrieved from: <https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity>
- Symantec. (2011). *W32.Duqu: The Precursor to STUXNET*. Retrieved from: [https://www.symantec.com/connect/w32\\_duqu\\_precursor\\_next\\_stuxnet](https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet)

- TWSG. (2005). Technical Support Working Group (TSWG): The Threat Of Radio Frequency Weapons To Critical Infrastructure Facilities. Retrieved from: [www.dtic.mil/dtic/tr/fulltext/u2/a593293.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/a593293.pdf)
- Vincent, C. H., Argueta, C. N., & Hanson, L. A. (2017, March 3). *Federal Land Ownership*. Retrieved from the Homeland Security Digital Library: <https://www.hsdl.org/?view&did=799426>
- White House. (2012). *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. Retrieved from: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- White House. (2017). *Cybersecurity Executive Order 13800: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Retrieved from: <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>
- White House. (n.d.). *Our Government the Executive Branch*. Retrieved from: <https://www.whitehouse.gov/about-the-white-house/the-executive-branch/>
- Williams, T. J. (1989). *A Reference Model for Computer Integrated Manufacturing (CIM): A Description from the Viewpoint of Industrial Automation*. Retrieved from: [www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.pdf](http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.pdf)
- Wu, T., Pagna Disso, J.F., Jones, K. Campos, A. (2013). *Towards a SCADA Forensics Architecture*. Retrieved from: <https://dl.acm.org/citation.cfm?id=2735340>
- Zetter, K. (2010). *Security Pros Question Deployment of Smart Meters*. Retrieved from: <https://www.wired.com/2010/03/smart-grids-done-smartly/>
- Zetter, K. (2012). *Meet 'Flame,' The Massive Spyware Infiltrating Iranian Computers*. Retrieved from: <https://www.wired.com/2012/05/flame/>
- Zetter, K. (2013). *Chinese Military Linked to Hacks of More Than 100 Companies*. Retrieved from [wired.com/2012/09/scada-vendor-telvent-hacked](http://www.wired.com/2012/09/scada-vendor-telvent-hacked).
- Zetter, K. (2014). *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon*. Broadway Books.