



**FIGHTING THROUGH A LOGISTICS CYBER ATTACK**

GRP

June 2015

Anthony R. Mollison, Maj, USAF

AFIT-ENS-GRP-15-J-027

**DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY**

**AIR FORCE INSTITUTE OF TECHNOLOGY**

**Wright-Patterson Air Force Base, Ohio**

DISTRIBUTION STATEMENT A.  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this dissertation are those of the author and do not reflect the official policy of the United States Air Force, the Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENS-GRP-15-J-027

**FIGHTING THROUGH A LOGISTICS CYBER ATTACK**

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Operational Sciences Graduate

School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Logistics

Anthony R. Mollison

Maj, USAF

June 2015

DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE;  
DISTRIBUTION UNLIMITED.

AFIT-ENS-GRP-15-J-027

FIGHTING THROUGH A LOGISTICS CYBER ATTACK

Anthony R. Mollison, M.S.  
Maj, USAF

Jeffrey A. Ogden, PhD  
Research Advisor

## **Abstract**

Cyber-attacks on information systems in the United States have steadily increased over the past decade. The true magnitude of these attacks was not revealed to the public until in 2013, the White House authorized the Federal Bureau of Investigation to notify over 3,000 companies in the private sector that their computer systems and networks had been compromised. These attacks are carried out by various types of criminal factions and foreign governments. The White House has directly accused China of orchestrating deliberate attacks on American government systems, to include defense contractors.

A cyber-attack on DoD information systems could severely degrade or disrupt the ability of the United States military to rapidly and effectively project decisive power against adversaries. The logistics enterprise is particularly vulnerable, given the scale of operations required to support the war fighter and its heavy reliance on unclassified networks.

This research focuses on The Global Air Transportation Execution System (GATES), managed by Air Mobility Command (AMC), which supports worldwide DoD transportation needs in peace and war by managing cargo and passenger information transiting through AMC aerial ports around the world. A cyber-attack on GATES could potentially degrade the force projection capability needed to meet operational requirements. This study shows how such an attack on GATES could potentially degrade the Air Force's ability to establish and sustain expeditionary base operations and meet sortie generation requirements. This study uses interviews and various documents to investigate the policies in place that provide guidance for the strategies and tactics, techniques and procedures (TTPs) that counter and mitigate such attacks on GATES.

AFIT-ENS-GRP-15-J-027

To my beautiful wife and our incredible children.  
Thank you for your unyielding support.

## **Acknowledgements**

I would like express sincere appreciation to my graduate research project advisor, Dr. Ogden, and to my sponsor, Mr. Dan Roberts for their support in the development of this research. Additionally, I would like to thank all the cyber and GATES subject matter experts who took time out of their busy schedules to educate me on the technical aspects of their respective fields. Last but not least, I would like to thank Air Force Materiel Command for funding the travels for the research of this topic.

Anthony R. Mollison

## Table of Contents

	Page
Abstract.....	iv
Acknowledgements.....	vi
List of Figures.....	ix
List of Tables.....	x
I. Introduction.....	1
<i>Background, Motivation and Problem Statement</i> .....	1
<i>Research Objective</i> .....	8
<i>Research Questions</i> .....	8
Strategic Level (SL):.....	9
Operational Level (OL):.....	9
Tactical Level (TL):.....	9
<i>Methodology</i> .....	9
<i>Assumptions/Limitations</i> .....	10
<i>Implications</i> .....	10
II. Literature Review.....	11
<i>The Evolution of Warfare</i> .....	11
<i>The Cyber Threat</i> .....	16
<i>Infiltrating GATES</i> .....	19
<i>SCADA Vulnerability</i> .....	22
<i>Fighting Through the Cyber Attack</i> .....	24
III. Methodology.....	27
<i>Data Sources</i> .....	27
IV. Analysis and Findings.....	30



	<i>Data Analysis</i> .....	30
	<i>Findings</i> .....	30
V.	Conclusions and Recommendations .....	39
	<i>Conclusions of Research</i> .....	39
	<i>Recommendations for Future Research</i> .....	40
	Appendix.....	43
VI.	Bibliography .....	44

## List of Figures

Figure	Page
1. GAO analysis of U.S.-CERT data for fiscal years 2012 – 2013.....	5
2. The share of world military expenditure of the 15 states with the highest expenditure in 2013 .....	6
3. How Stuxnet Works.....	15
4. Victim countries most affected by cyber espionage in 2013, by share of incidents.....	17
5. System Network: Information Exchanges Between Logistics IT Systems .....	29
6. Process Owner Network: Information Exchanges Between Process Owners .....	29
7. 624 OC Lines of Effort .....	34

## List of Tables

Table	Page
1. Evolution of Weaponry.....	12
2. Focus of Cyber Logistics Systems by command level .....	30

# FIGHTING THROUGH A LOGISTICS CYBER ATTACK

## I. Introduction

*“Adversaries of the United States constantly seek to infiltrate networks and degrade capabilities, disrupt operations, or steal information.”*

- General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff

### ***Background, Motivation and Problem Statement***

Joint Pub 3-13: Information Operations defines Cyberspace as: “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Joint Chiefs of Staff, 2014).

Cyberspace is a ubiquitous domain that can be found in almost every facet of our lives. This immense assembly of networks, which was developed to provide scientists around the world a platform to share information and computing power, has expanded to include personal computers, fiber optics, routers, switches and mobile devices. Today, it is used to manage personal and industrial finances, monitor and operate our power grids, control our transportation nodes, and distribute various forms of entertainment any time of the day...on demand. There isn't an industry in the modern world that does not utilize cyberspace in some form to conduct its daily operations or to communicate with other companies internal or external to its industry. Although there is sufficient evidence to support the plethora of advantages cyberspace has brought to commercial entities and the government sector, the same inherent ease of use and initial economical accessibility provides agents with maleficent tendencies the opportunity to interfere with productivity in the form of attacks.

Over the past decade, activity over cyberspace has increased exponentially. Its borderless nature provides businesses of all sizes an equal playing field in which they can receive and exchange information near real-time. Government agencies also utilize the cyber domain to rapidly disseminate and exchange information for the security and defense of their respective organizations. As the use of and dependence on cyberspace has steadily increased, so has the appetite for exploiting the vulnerabilities of the information systems it supports.

In 2011, Norton of Symantec, a leading manufacturer of anti-virus software and cybersecurity suites published a report on the economic impact of cyber-attacks (Symantec, 2011). The report findings revealed that over the previous year, 431 million adults in 24 countries were victims of cyber-attacks at a financial loss of \$114 billion. The value of productive time lost as a result of the cybercrime was estimated to be \$274 million. The report added that the cumulative cost of cyber-attacks was more than the combined global black market cost of cocaine, heroin and marijuana. These alarming figures raised international concern leading to the United Nations Economic and Social Council (ECOSOC) to convene a Special Event on “Cybersecurity and Development” just three months after the report was published. During the event, the United Nations estimated the global impact of cyber-attacks in 2011 exceeded over \$1 trillion dollars (United Nations, 2011).

Cyber-attacks on information systems in the United States have steadily increased over the past decade. The true magnitude of these attacks was not revealed to the public until in 2013, the White House authorized the Federal Bureau of Investigation (FBI) to notify over 3,000 companies in the private sector that their computer systems and networks had been compromised (Nakashima, 2014).

Businesses and government agencies alike have become increasingly reliant on automated systems working over the cyber domain. While the benefits of its use have been very rewarding, its ease of use and access has created vulnerabilities that when exploited, create significant damage. The culprits of these attacks range from various types of criminal factions (including both independent and organized groups) to foreign government proxies. Such groups claimed responsibility for cyber-attacks on US businesses and government agencies in 2014, which impacted millions of customers and caused millions of dollars in damages. In many cases the attacks are so severe and obscure that the damages are not easily quantified. In his first televised interview, in an effort to explain the severe climate cyberspace is in currently, FBI Director James Comey stated on CBS 60 Minutes: “there are two types of big companies in the U.S., those that have been hacked...and those that don’t know they have been hacked” (Cook, 2014).

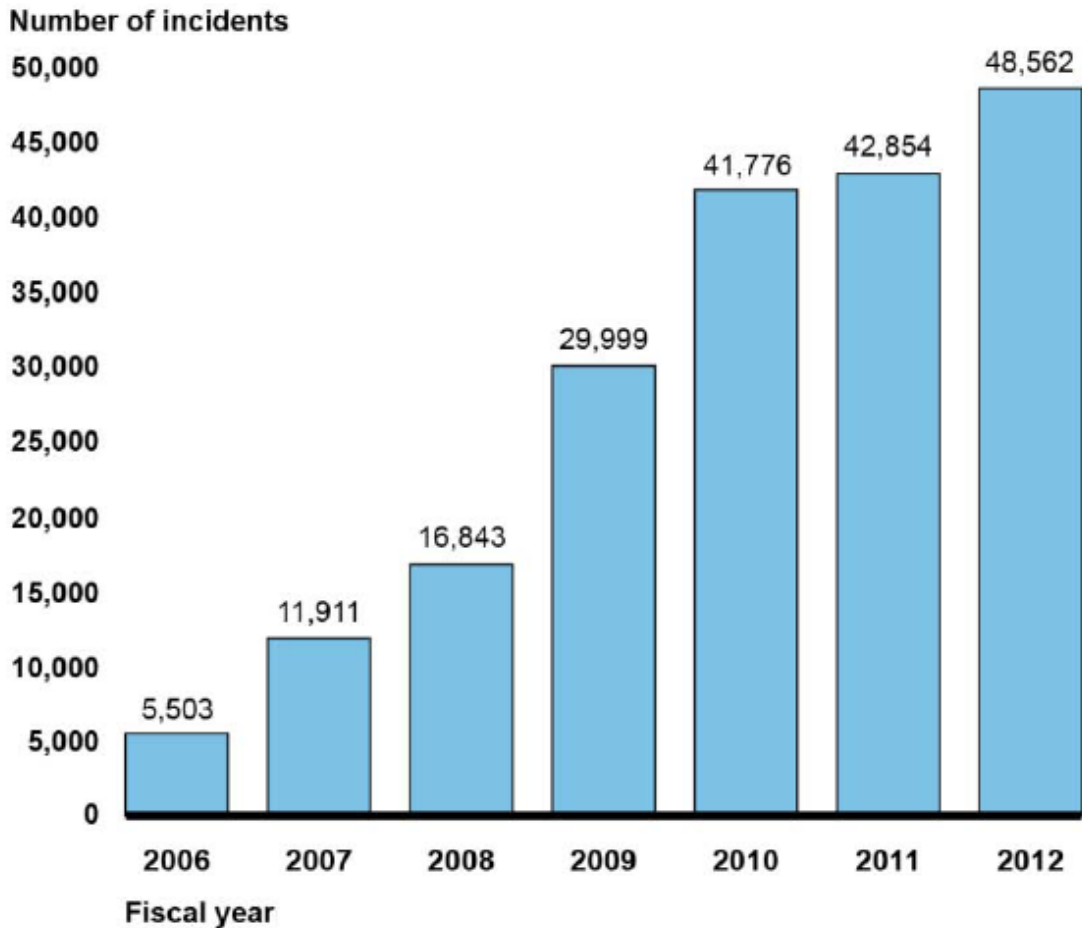
A well-coordinated attack on the U.S. could severely impact the economy, health services, transportation, homeland defense and ultimately degrade military capability. U.S. security firm Mandiant (2013), published a report linking the Chinese military to most attacks on U.S. business and government agencies such as the Department of State and U.S. Transportation Command (USTRANSCOM). Following the report, The White House publicly accused China of orchestrating deliberate attacks on American government systems, to include defense contractors (Sanger, 2013).

Information Technology (IT), as defined by the Clinger-Cohen Act of 1996, sections 5002, 5104 and 5142, means any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement,

control, display, switching, interchange, transmission, or reception of data or information (Office of Management and Budget, 2008).

IT systems enable organizations to rapidly share massive amounts of information (in many cases real-time) among many users at a very low cost. The number of networks the DoD uses to execute its mission has increased exponentially over the past decade. These systems have revolutionized daily operations so much that the DoD has implemented policies to become more paperless (a term used to describe a process that is completely done on a computer or online). Although there is evidence of increased productivity and efficiency in managing, sharing and storing of information, the use of IT has left the DoD highly dependent on these systems to conduct even the simplest tasks (United States Government Accountability Office, 2013).

As Figure 1 show, the number of reported incidences on government systems over the past four years. Unfortunately, the number unreported or undocumented incidences will never be known. A successful cyber-attack on DoD information systems could severely degrade or disrupt the ability of the United States military to rapidly and effectively project decisive power against an adversary.



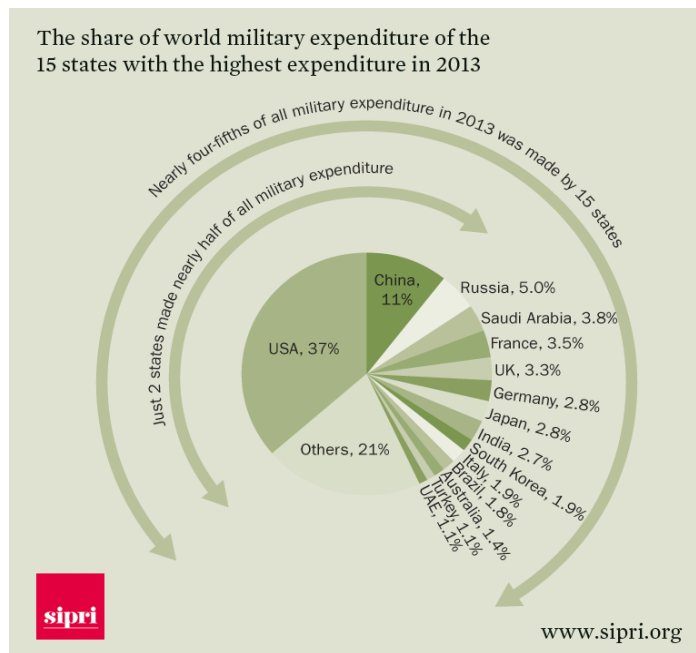
**Figure 1: GAO analysis of U.S.-CERT data for fiscal years 2012 – 2013** (United States Government Accountability Office, 2013)

DoD’s IT infrastructure enables warfighters to operate more efficiently in today’s modern warfare. In 2008, the DoD defined cyberspace as one of the five warfighting domains along with land, maritime, air and space (Williams, 2011). Logistics IT systems have a significant role in all five of the Air Force core missions: Intelligence Surveillance and Reconnaissance (ISR), Air and Space Superiority, Rapid Global Mobility, Global Strike and Command and Control (C2). Logistics IT systems have a particularly prominent role in the employment of Rapid Global Mobility and C2. Given the scale of logistics operations required to support the modern war fighter, the heavy reliance on unclassified networks makes the entire logistics enterprise



vulnerable to cyber-attacks. The Global Air Transportation Execution System (GATES), USTRANSCOM’s port automation system that supports movement of cargo and personnel around the world, is especially susceptible to such an attack.

The U.S. military budget makes up over 37 percent of all the military budgets in the world, as depicted in Figure 2. A large portion of this budget is allocated to securing our critical assets for DoD operations abroad and in the defense of the Homeland. Unfortunately, many of the facilities and infrastructure that support our most vital IT systems are not adequately protected; there isn’t sufficient guidance, or funding allocated to the security of our Supervisory Control and Data Acquisition (SCADA) systems which is a core component to any system or enterprise.



**Figure 2: The share of world military expenditure of the 15 states with the highest expenditure in 2013 (Stockholm International Peace Research Institute, 2014)**

A clever adversary may be less inclined to employ a direct cyber-attack against a vital system such as GATES, and instead focus her efforts on a less secure more conspicuous system

such as the SCADA systems that support GATES. The operation of GATES depends on numerous military and civilian SCADA systems. An effective attack (which does not require a high level of expertise), could have a significant impact on the U.S. military's ability to operate or meet mission requirements.

Another area of concern is our commercial contractors. The DoD's increased use of commercial contractors is a result of the reduction in force which is focused on retaining only positions that are expeditionary and believed to be more relevant to future wars (i.e. special operations and cyber) (Sanchez, 2014). Thus, most support functions have been delegated to contractors who are trusted with a large quantity of sensitive information in order to fill a capability void. Quite often we find the security protocols in these companies are not as stringent as those the DoD mandates on itself. Presently, the DoD does not have policies in place to determine whether contractors are meeting required standards. This is obviously an area of concern.

Just as the U.S. conventional military has been an effective deterrence from a conventional frontal attack, the U.S. "conventional" cyber capabilities can provide a similar result. It is very unlikely that an adversary is going to orchestrate a direct cyber-attack on our logistics IT systems. That is not to say that a capable adversary does not exist. On the contrary, nations such as China, North Korea and Russia have the demonstrated capability of such an attack (Sanger, 2013).

The most probable course of action may be to attack a supporting infrastructure that acts as a critical capability/requirement that may disrupt or degrade the system's capability. This paper will show the most probable method of cyber-attack a capable adversary may take to disrupt or deny access to GATES, which may lead to the degradation of the Air Force's ability to

establish and sustain expeditionary base operations and meet sortie generation requirements (Zimmerman, Norris, & Frasier-Loria, 2014).

### ***Research Objective***

This project will focus on The Global Air Transportation Execution System (GATES), managed by Air Mobility Command (AMC), which supports worldwide DoD transportation needs by managing cargo and passenger information transiting through AMC aerial ports around the world. A cyber-attack on GATES could potentially degrade the force projection capability needed to meet operational objectives. This study will show how such an attack on GATES could potentially degrade the Air Force's ability to establish and sustain expeditionary base operations and meet sortie generation requirements. This study will also investigate the policies in place that provides guidance for the strategies and TTPs that counter and mitigate such attacks on GATES.

This project examines the relevant cyber threats against GATES. A collection and analysis of open source data will be used to conduct this study. Once a most likely type of threat is selected, an assessment of the impact such an attack would have on combat operations would have been derived.

### ***Research Questions***

The following questions were presented to organizations at the strategic, operational and tactical level of command that are affiliated with GATES as a(n) program manager, operator, training manager or network systems administrator, for their respective views on how the Air Force would to fight through a compromised GATES:

Strategic Level (SL):

- 1) Are there any Air Force policies and guidelines for safeguarding logistics IT systems when operating in cyberspace?
- 2) Are cyber warfare officers and NCO's approach to training focused to defend logistics systems?
- 3) How does the Air Force plan to prepare logistics forces to work in a cyber contested environment?

Operational Level (OL):

- 1) What guidelines are given logistics units to defend their systems against a cyber-attack?
- 2) What is the most probable form of attack against a GATES?
- 3) Are other military services, government agencies and contractors that utilize GATES held to the same security protocols as Air Force systems on the AFNET?

Tactical Level (TL):

- 1) Are GATES operators (non-cyber personnel) trained to recognize a cyber-attack on the system?
- 2) What procedures are in place to mitigate an attack on GATES
- 3) How many people and man-hours does it require to operate in an environment absent of GATES?

***Methodology***

The researcher worked with 24AF and AMC/A4 to identify how GATES is associated with commercial firm information systems. AMC/A6 was sought out to explain the technical aspect of attacks and defensive measures AMC have implemented against such attacks.

Additionally, various CONUS and overseas aerial ports were visited to conduct interviews and analytic review of current TTPs and standing operating procedures (SOPs) that are in place to mitigate any disruption of GATES during combat operations.

### ***Assumptions/Limitations***

Much of the information regarding this topic is classified SECRET or higher due to the sensitivity of the topic. The focus of this research will be on the Non-Secure Internet Protocol Router (NIPRnet), which has shown to be more susceptible to an attack for reasons that will be discussed in this study.

### ***Implications***

The findings of this research will guide identification of agile Combat Support (ACS) capability and capacity gaps to influence Program Objective Memorandum (POM). This research will be used to inform tactics, techniques, and procedures (TTPs) for implementation within the GATES and other transportation logistics systems, for continuation of global logistics support in the face of cyber-attacks. Identification of threats and impacts are key to issuing guidance and policy that will mitigate and minimize the impact of any adversarial cyber threat. We anticipate such TTP and Policy changes could result in significant benefits to COCOMs.

## **II. Literature Review**

### ***The Evolution of Warfare***

Throughout human history, the need for devices to overcome physical limitations has led to the development of innovative devices to incorporate into daily lives. Some devices drastically improved the living conditions of those who possessed them; at times making them more prosperous than those who did not possess the device. As populations grew and resources became less abundant, so did the escalation of conflict between those who had and those who did not have. In simple terms, people have gone to war for two main reasons: to better their lives or to protect their way of life.

Since the beginning of human conflict, the quest to design a device (later to be called a weapon) that will give a superior advantage over an adversary has always been conducted in parallel with the altercation. Military theorist Carl von Clausewitz coined this: causing the culmination of the opponent or bringing them to the point where they lose the ability or/will to fight (Clausewitz, 1989).

Over the centuries, communities, tribes and nations looked upon technology to provide a “culminating” weapon to give an overwhelming advantage over an adversary. Table 1 highlights some of the weapons that drastically changed the way battle has been waged. This list is not all inclusive as there are many other weapons throughout history that had a significant impact on the way war was waged, such as the submarine, self-loading rifles and precision guided munitions just to name a few.

Table 1: Evolution of Weaponry

3000 B.C. – 1700 B.C.	Chariot
800 - 1350	Gunpowder
1915	Machine Gun
1915	Tanks
1915	Aircraft
1935	Radar
1945	Nuclear Weapons
1960	Satellites
1989	GPS
2009	Cyber Weapon

Prior to the Egyptian’s introduction of the chariot, wars were waged primarily on foot. This horse driven cart added incredible speed on the open battlefield and imposed a great advantage over the opposing pedestrian force.

Although the Chinese may have invented gunpowder as early as 800 A.D., its capability was not fully exploited until early in the 20th century when combined with the development of the machine gun. Many will argue the acquisition of gunpowder by western Europeans from the Chinese contributed to Western Europe’s domination of most of the world (Grossman, 2015).

The aircraft and the tank made their battlefield debut during World War I. Although both technologies were still in their infancy, the technologies convinced future pioneers George S. Patton and Billy Mitchell of their potential. Both men would go on to exploit the capabilities of their respective platforms during WWII and cement their legacy in history.

The British development of the radar is a perfect example of the proverb, “necessity is the mother of invention”. This technology became operational at a point in the war when the German air force, The Luftwaffe, nearly brought the country to its knees. The Luftwaffe was uncontested in the Battle of Britain until radar’s ability to detect inbound aircraft provided the British sufficient warning to launch intercepting aircraft and challenge the Luftwaffe (Nasr, 2015).

Noted by many as the most devastating weapon ever created, the nuclear weapon was introduced to the world in 1945 when the U.S. detonated it over the cities of Hiroshima and Nagasaki, Japan. This weapon unleashed a force so lethal and devastating, it instantly killed tens of thousands of people and several hundred thousand more through a slow agonizing death caused by the effects of thermal burns and radiation poisoning (Atomic Bomb Museum, 2006).

The space race facilitated the creation of many new technologies. Advancements in propellants and rocket engineering paved the way for the development of satellites. These instruments coupled with the advancement in communications, provided the capability to actively and passively collect vast quantities of information on an adversarial nation 24 hours a day without the limitations and risks a manned aircraft would endure. The Global Positioning System later followed in 1989, providing precise navigation and accurate targeting. Combined with satellites, they are able to accurately map any terrain on the planet.

The birth of the Internet can be traced back to 1962. Advanced Research Projects Agency (ARPA), a technological think tank organization made up of scientists whose initial focus was on space, ballistic missile and nuclear test monitoring, had a vision to develop the ability for computers to communicate between its operating base and its sub-contractors. By 1967, unbeknownst to each other’s efforts, ARPA and teams from the Massachusetts Institute of

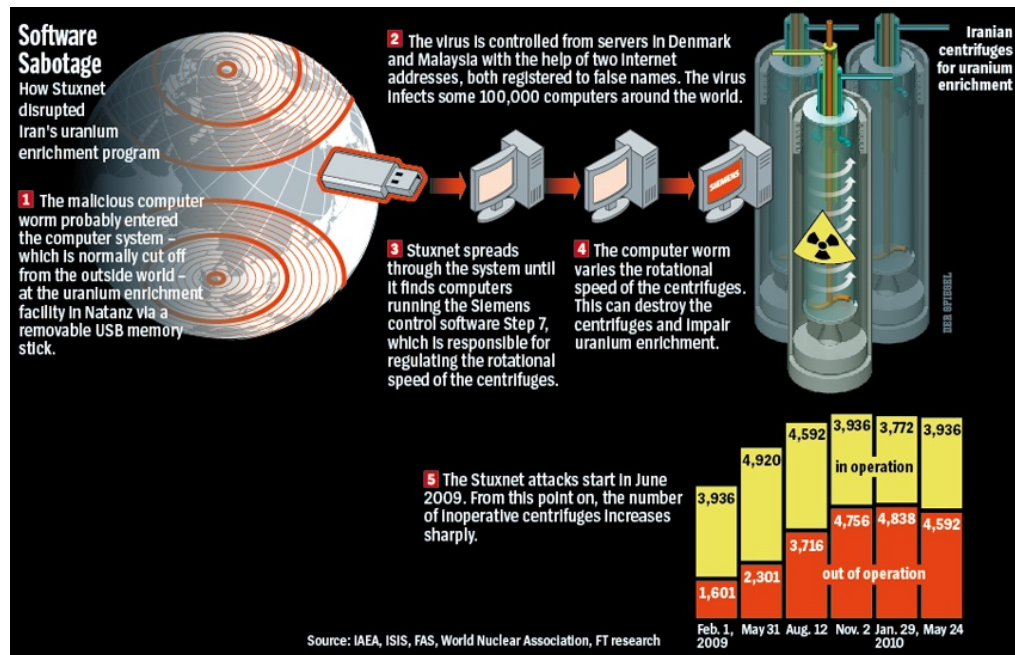


Technology (MIT), the National Physics Laboratory in the United Kingdom and RAND Corporation had all been working on the development of a wide area network. The teams successfully incorporated their efforts and created ARPANET. In December 1969, ARPANET successfully developed a network of four computers. Three years later ARPANET went public and grew to a network consisting of host computers from 40 different locations. This network primarily remained in the scientific and academic communities for the next 22 years (Griffiths, 2002).

The Internet as we recognize it today came to fruition in 1991 after ARPANET was dissolved as a government entity and surpassed by the rapid expansion of the commercial sector. The enactment of the High Performance Computing Act of 1991, led by then Senator Al Gore, enabled the development of the World Wide Web (WWW or the Web). Griffiths (2002), defines the Web as an abstract space information containing hyperlinked documents and other resources, identified by their Uniformed Resource Locator (URLs). It is implemented as both client and server software using Internet protocols such as transmission control protocol/internet protocol (TCP/IP) and Hypertext Transfer Protocol (HTTP) (Griffiths, 2002).

The simplification of the Internet made computing and access to cyberspace less obtrusive and more attractive to a large number of people. Today cyberspace has been incorporated into nearly every aspect of our daily lives (i.e., personal and industrial finance management, monitor and operate power grids and other critical infrastructure, control of transportation nodes, homeland security and defense). Over the past decade, this reliance on cyber has given birth to a new category of crime (cybercrime) in which criminals use cyberspace to extract, distort or manipulate sensitive information from individuals, businesses or government organizations (Department of Homeland Security, 2013).

The first successful deployment of a cyber-weapon is believed to have occurred in 2009. Stuxnet (as it later came to be known), is a complex malware virus that is believed to have been a joint U.S./Israel operation to target and sabotage the Iranian uranium enrichment process at the Natanz facility (Finkle, 2013). Figure 3 graphically shows how Stuxnet sabotaged the uranium plant at the Natanz facility.



**Figure 3: How Stuxnet Works (Stark, 2011)**

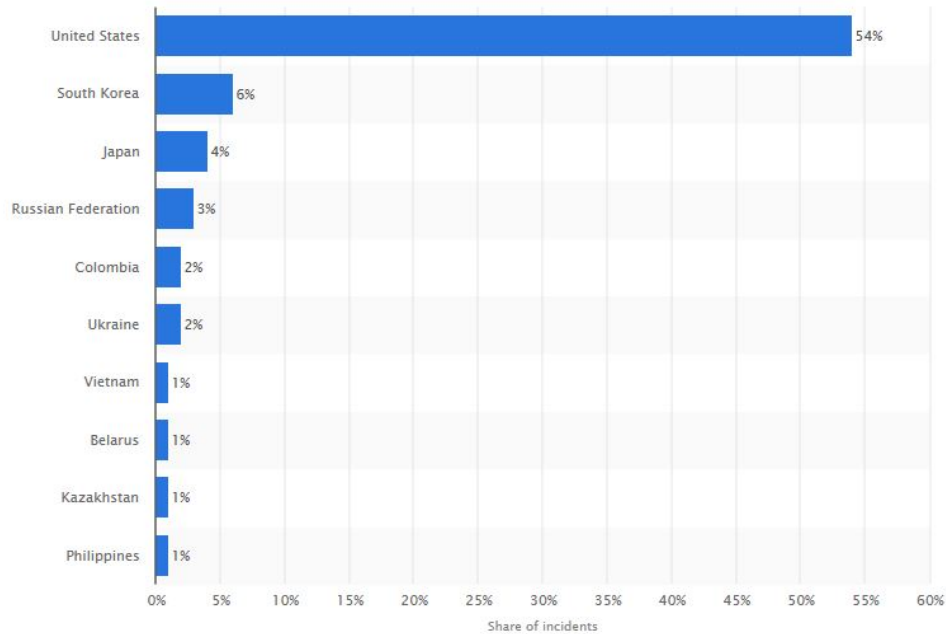
The virus concealed its origin by rerouting itself on over 100,000 computers around the world (60,000 of which were inside Iran). Stuxnet was designed to target a specific program (industrial control software named Step 7), developed by the Germans that controlled the centrifuges. The attack was so subtle that it went unnoticed by the operators at the facility for an unspecified period of time. Its complexity and sophistication was unprecedented to date, thus, introducing a new era of warfare where a non-kinetic attack on a system successfully caused devastating results (Stark, 2011).

## *The Cyber Threat*

It has become common in recent news to hear a company has been hacked by criminals who illegally gained access to a vast amount of sensitive data. A large proportion of the cyber-attacks around the world target U.S. companies and government agencies. This may be due to the abundance of intellectual property and technological advancements originating in the U.S.

McConnell points out that most attacks on the U.S. cyber infrastructure, both civilian and military, tend to focus on data exploitation rather than destruction. Foreign governments are more inclined to gain access to data for intelligence on technology or military capability, while criminals seek data for financial gain. However, cyberterrorists seek gain access to systems to destroy or corrupt the data. The two very different goals often are mistakenly combined when people consider cyber threats (Ackerman, 2008). As figure 4 shows, there is a growing appetite for unauthorized access to U.S. IT systems by state and non-state actors. Ultimately, it is the end user who is first line of defense.

The culprits behind these attacks range from criminal factions (an individual or organized group) or a state sponsored organization. Government and independent studies show that the majority of attacks point to China and Russia as the prime suspects. However, the origin of the attacks is traced to within the U.S. Clever hackers have resorted to disguising their origin by gaining access to command and control (CnC) servers from within the U.S. in an effort to mask their origin and exfiltration without a trace (Constantin, 2013).



**Figure 4: Victim countries most affected by cyber espionage in 2013, by share of incidents (Statista, 2015)**

An example of such an attack that is designed to infiltrate a target’s system and linger in the background until a predesignated time is the malware named “Flame”, discovered by the Russian anti-virus firm Kaspersky Lab. The firm discovered the malware in 2012 and is said to have infiltrated systems in Iran, Lebanon, Syria, Sudan, the Israeli Occupied Territories and other countries in the Middle East and North Africa for at least two years before being discovered (Zetter, 2012).

The threat is vastly growing in the number of incidences and complexity. According to the Global State of Information Security Survey 2015, the compound annual growth rate (CAGR) of detected incidences (cyber-attacks) rose 66% year over year since 2009. The majority of incidences were detected by large companies grossing over 1 billion dollars in revenue. Two assumptions can derive from this: 1) larger companies have the resources to invest in more sophisticated cyber security, thus detect more intrusions; 2) hackers target these

companies more because of the abundant intellectual and financial assets they possess (e.g., consumer data, corporate information) (PWC, 2014).

Although many of these companies have taken measures to fortify and protect their IT systems, the report finds that 71% of security breaches go undetected. The more creative attackers will infiltrate the most complex defenses by targeting the networks of smaller companies who do not have robust resources to defend their systems or they lack the security protocols that the larger companies incorporate to their daily operations. The attacks on the smaller companies provide a circuitous but equally effective access to the larger companies (the true target) that are interconnected with them (PWC, 2014).

It is very probable that the aforementioned scenario is the most likely method an adversary will use in an attempt to gain access to GATES. The ubiquitous nature of GATES with over 14 thousand users connected over the World Wide Web makes it a very appealing target. In fact, GATES becomes more vulnerable each time it interfaces with a *.com* domain name system (DNS).

This has prompted the U.S. to take a closer look at its current scope of capabilities while establishing TTP's to avert future threats. Attackers have demonstrated the will, skill and patience to attack network systems through alternative means such as social media outlets. The threats have progressed beyond attacks against common administrative networks and websites as evident by the January 12, 2015 hacking of U.S. military's Central Command social media accounts by a hacking group named Cyber Caliphate, claiming allegiance to the Islamic State. Although military officials are ruling the incident as mere "cybervandalism", it sends a clear message that U.S. adversaries are constantly prowling and lurking in the shadows looking for vulnerabilities in our systems. (Lamothe, 2015)

## ***Infiltrating GATES***

The computer systems used in the workplace are no longer towering on a member's desk or gracefully hidden under a desk. Today's computers are cleverly called laptops or notebooks because of their size and portability. These attributes make them convenient to take home or on business trips. Additionally, mobile devices such as smart phones and tablets have increased in popularity as their computing capability continues to mature. Many of these computers and devices are Wi-Fi and Bluetooth compatible, which enables them to remotely access applications on their home station's local area network (LAN) via a virtual private network (VPN) (Rietscha, 2012).

Many service members while on temporary duty (TDY) will use their Wi-Fi enabled laptops and mobile devices to access the network at airports or hotels. This is a prime opportunity for an attacker. The defensive protocol networks at many hotels are not fortified with robust defensive capabilities, thus becoming a soft target (Castrodale, 2015). Once the member returns the device to the host installation and reconnects to the installation's network, the concealed threat has the ability to access and map the network undetected until it is ready to strike (Buley, 2008).

Early versions of Bluetooth phones and devices were known for having security vulnerabilities. Although many of these gaps have been corrected by the manufactures, some still remain. Bluesnarfing (the access of information through Bluetooth) and bluejacking (sending unsolicited messages and controlling of a device) attacks can take over devices through a Trojan horse program. This method is highly technical; it requires sophisticated hardware, software and a highly skilled hacker more commonly found among professional spies or state sponsored actors (624th OC, 2014).

Another clever and more surreptitious method used to gain access to a network is through the use of social engineering. Social engineering is defined as a non-technical method of intrusion a hacker uses that relies heavily on human interaction in order to influence and deceive people and take advantage of their misplaced trust in order to obtain insider information (Lenkart, 2011).

Kevin Mitnick, a world renowned hacker, testified before the Senate Governmental Committee in March 2002 on his ability to easily gain access and circumvent security measures to some of the largest corporations in the world by use of social engineering. Mitnick further emphasized how many of his greatest conquests were accomplished with minimal hardware and software capabilities. The information he received through social engineering tactics enabled him to bypass some of the best information security measures in the industry from companies such as AT&T, Nokia and Motorola (2600 News, 2000).

Social networking sites (SNS) such as Facebook, Skype, Twitter and YouTube provide a creative outlet for people. In other cases it provides a forum for the exchange of ideas or simply to keep in touch with friends and loved ones. Social engineers survey these outlets in search of a conduit or proxy to gain access to their next target. Some of the tactics used seemed innocuous but are cleverly crafted with a definite end state in mind. The attacker will gather information by asking simple questions over time carefully not overstepping to avoid alarming the victim. The questions will provide key information about the company or organization and its network such as: scheduled outages, names of key IT personnel and senior management, which over time will enable the attacker to piece together all the information required to formulate an attack at a time of his choosing (Lenkart, 2011). The most sophisticated defensive measures on a network are

useless if the keys to the proverbial door are handed to the intruder. Ultimately, the end user is the weakest link in our defensive system.

In 2009, Thomas Ryan, co-founder of Provide Security LLC drew the attention of the world when he revealed the results of a 28 day social engineering experiment he conducted named Robin Sage. Robin Sage is a fictitious persona that was to engage with U.S. military personnel through social networking with the goal to obtain information from them. Sage was able to make contact with men working for the chairman of the Joint Chiefs of Staff, the National Reconnaissance Office (NRO), which oversees the development and launches of U.S. spy satellites, the chief of staff for a U.S. congressman, and several senior executives at defense contractors, such as Lockheed Martin Corp. and Northrop Grumman Corp. Most of the individuals were seasoned security professionals (Lisko, 2010).

The Sage experiment successfully identified how harmless details via social networking sites could be destructive to both an individual's protection and corporation's security. Ultimately, it is up to the individual end user to ensure the security of a network. Although any network is capable of being breeched given the time and resources, it is much more challenging for an attacker to gain access to a system without trusted access.

The Logistics Module (LOGMOD) is a computer software program that runs on computers at both the MAJCOM and base level through networked servers. It is used to manage a database containing the logistics equipment and supplies for Air Force Unit Type Codes (UTCs). Deploying unit cargo information is consolidated in LOGMOD and passed via file transfer to CMOS/GATES by the Plans and Integration Section within the Installation Deployment and Reception Center and the Deployment Control Center (IDRC/DCC) to provide ITV to Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence



(IGC). This is a key vulnerability that may provide access to GATES through an unaware user who is not directly working on GATES.

A skilled hacker does not require an extensive knowledge in logistics. A skilled hacker will patiently observe the activities on the network they infiltrated to learn the processes and procedures of the organization as well as other systems that communicate with the system. Once the hacker acquires sufficient knowledge of the system's capability, purpose and vulnerabilities, the hacker then determines how to unleash the attack or further exploit the system (McGuiness, 2011). A penetration of this sort on GATES could seriously impede the operation of U.S. forces during a contingency by degrading network connectivity, corrupting data and providing intelligence to the adversary.

In a study conducted by the Idaho National Laboratory on Air Force Industrial Control Systems (ICS), Air Force IT systems have formed colossal web linking various systems previously not related to become more efficient. This interdependency on various systems enabled each of these systems to become more vulnerable to disruptions due to intentional and unintentional cyber-attack from a periphery such as a supporting infrastructure. Supporting infrastructure may be a critical capability susceptible to attack that may disrupt or degrade the system's capability.

### ***SCADA Vulnerability***

Joint Publication 5.0 defines a Center of Gravity (COG) as “a source of power that provides moral or physical strength, freedom of action, or will to act...” It is what Clausewitz called “the hub of all power and movement, on which everything depends.” The U.S. military is certainly a COG by this definition. The U.S. military is recognized as the most powerful military force in the history of the world. It has secured the sea lanes enabling global trade, thus,

sustaining a robust economy. Additionally, it has been an effective deterrent from an overt military attack from another nation for over 70 years.

The U.S. military's dependency on IT systems and the cyber domain to conduct war are critical capabilities as defined by Joint Publication 5.0: "critical capabilities are those that are considered crucial enablers for a COG to function as such, and are essential to the accomplishment of military objectives" (Joint Chiefs of Staff, 2011). U.S. adversaries are aware of this fact. The frequency of attacks on U.S. military IT systems supports this fact.

A Supervisory Control and Data Acquisition (SCADA) system is an industrial computer system (ICS) used for monitoring industrial infrastructure such as utilities (in particular power grids) and communications systems. As mentioned previously, U.S. formidable cyber capabilities encourage adversaries to divert their focus on softer targets. It is very probable that an adversary will seek a peripheral, yet critical capability that is vital to the sustained operability of GATES that is not heavily defended. SCADA systems fit the profile of such a target.

The Department of Homeland Security reported in 2009 that the SCADA systems that control the nation's power grids are not adequately protected from a cyber-attack (Piggin, 2010). The U.S. critical infrastructure comprises of 16 sectors that provide vital services essential to our society such as: Communications, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Nuclear Reactors, Waste and Transportation Systems (Zimmerman, Norris, & Frasier-Loria, 2014). Many of the U.S. military installations in the U.S. and overseas are serviced by SCADA systems managed by the local municipality.

Many of the SCADA systems that monitor and control the U.S. critical infrastructure have been in operation for up to 30 years. These systems were designed to be proprietary stand-

alone networks, which were later haphazardly connected to the Internet without the proper security measures. Although many of these systems have been updated with increased automations, much of it is still under human control, which renders it susceptible to the natural latent response of human input in an automated environment and the potential of human error during an emergency (Massoud, 2010).

Additionally, the systems are not designed to automatically receive automatic updates such as security patches. They are sometimes not supplied to end-users, or are supplied but not installed to the system for fear of negatively impacting system performance. Much time is wasted due to the current practice of installing security patches only after SCADA vendors have thoroughly tested the system, leaving the system vulnerable to current threats (Massoud, 2010)

### ***Fighting Through the Cyber Attack***

GATES is the IGC Intransit Visibility (ITV) feeder system used by Air Mobility Command (AMC) aerial ports and deployed forces to process, manifest, and track passengers and cargo, support resource management and provide command and control support information. It is also part of an automated family of systems known as Integrated Deployment System (IDS) that is comprised of LOGMOD, DCAPES, CMOS, and ICODES that are used for wing-level deployments and contingency operations. Failure to use the full capabilities of IDS hinders an installation or a wing's ability to achieve timely ITV and will reduce the combatant commander's (CCDR's) visibility to track force closure (Air Mobility Command, 2014).

Aerial Ports are encouraged to use GATES and all other automation tools to the maximum extent possible. Automation tools such as GATES save time, resources and maintain data integrity. In the event of loss of automation, there are protocols in place to work around a disruption of GATES. AMC Instruction, 24-101, Volume 22, Air Transportation Training

Requirements mandates that manual procedures are to be exercised at least quarterly and when possible, to be in conjunction with wing exercises. Many aerial ports have Standard Operating Procedures tailored to their unique units for operating in an environment absent of GATES capability. Volume 9, Air Terminal Operations Center, gives guidance on the procedures for operating an Air Terminal Operations Center (ATOC) without GATES capability as well as outside agencies not equipped with GATES (Air Mobility Command, 2012).

It must be noted that none of the 24 series AFI's (Transportation series) to include the aforementioned above address the possibility of an environment absent of GATES as a result of a cyber-attack. In the event GATES is not operational, members are instructed to contact the GATES help desk and coordinate any backlog with TACC/XOGB. The main objective of operating an aerial port during a GATES outage is to ensure all aerial port functions continue uninterrupted, to include capturing all data required for reporting to higher HQs, lateral units and down-line units. However, unit SOP's do not address cyber-attack as a possible cause for disruption. The closest reference to an attack on the system is in AMC Instruction, 24-101, Volume 14, where it states: "automated data processing (ADP) or computer equipment failure" as a cause for inoperability. Information of such an attack can be critical for the situational awareness of the other units connected to the network. This may provide them the cognizance to seek out similar patterns in the disruption that may prove vital for cyber professional's assessment of the situation.

Operating an aerial port without GATES or with data that has been manipulated can have a negative impact on the CDR's ability to prioritize cargo and personnel to meet his/her intent. In coordination with CDRUSTRANSCOM and other supporting commanders, the CDR is responsible for the movement of cargo and personnel into her area of operation (AOR) in an

effort to meet his/her campaign objectives. The schedule of these requirements is scripted in the Time Phased Force Deployment Data (TPFDD), a planning document that originates in JOPES and then transferred to GATES via an interface with Deliberate and Crisis Action Planning and Execution Segments (DCAPES) (Joint Chiefs of Staff, 2013). Once the requirements are in GATES, the CCDR has two processes at to use at his/her discretion to quickly move cargo through the transportation system. They are the Green Sheet and Purple Sheet process.

The Green Sheet process is not a priority; it is designed to override priorities when expedited movement of shipments is considered to be in the interest of national defense. On the other hand, the Purple Sheet process authorizes specific cargo identified in the AMC system in transit to the Combatant Command (COCOM) to be of operational necessity (Air Mobility Command, 2014). Any degradation or manipulation of the data in GATES will make this already challenging endeavor more cumbersome and subject to human error especially during high ops tempo such as Phase 2 of a theater campaign or a Crisis Action situation.

Using the literature, the extent of the reach of cyber has been emphasized in an effort to paint a picture to the reader. The cyber threat is ever-present and ever evolving, requiring the Air Force to constantly expand beyond its current scope of capabilities. To defend a network effectively, a cyber-warfare team must understand both the technologies that comprise the network and the function it performs (i.e., the mission it supports) (Franz, 2011).

### **III. Methodology**

#### ***Data Sources***

This study supplements previous and existing projects aimed at improving the defense of USTC and AMC logistics systems that are heavily reliant on the dot com domain to conduct their mission. In an effort to get a full understanding of the impact of cyber-attacks on Air Force logistics systems, interviews were conducted with cyber and GATES experts at the strategic, operational and tactical levels of command.

In order to better understand Air Force strategic cyber policies and command structure, interviews were conducted with members of U.S. Air Force Headquarters, A3/6 (USAF HQ A3/6). Additionally, USAF HQ A3/6 detailed U.S. Air Force's role in the Comprehensive National Cybersecurity Incentive (CNCI) efforts to defend the U.S. information and communications infrastructure.

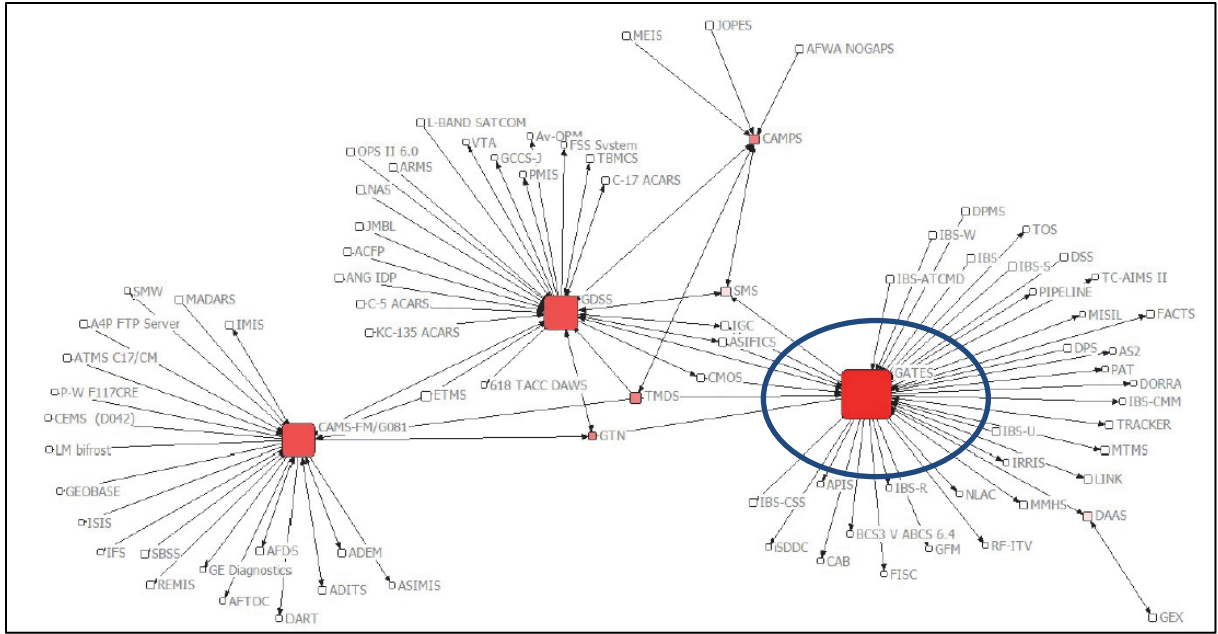
This research only examined the unclassified vulnerabilities of GATES that can be referenced back to open sources. To better understand the challenges of working in cyberspace and the operational vulnerabilities Air Force members must overcome while conducting their daily activities, interviews were conducted with cyber experts from the 24th Air Force and 624th Operations Center.

In an effort to learn more about vulnerabilities specific to AMC's logistics systems, interviews were conducted with members of AMC/A4, who identified how GATES is associated with commercial firm information systems. AMC/A6 explained the technical aspect of attacks and defensive measures AMC has implemented in coordination with the 624th OC against such attacks. Additionally, members of the Cyber Threat Working Group (CTWG) provided an

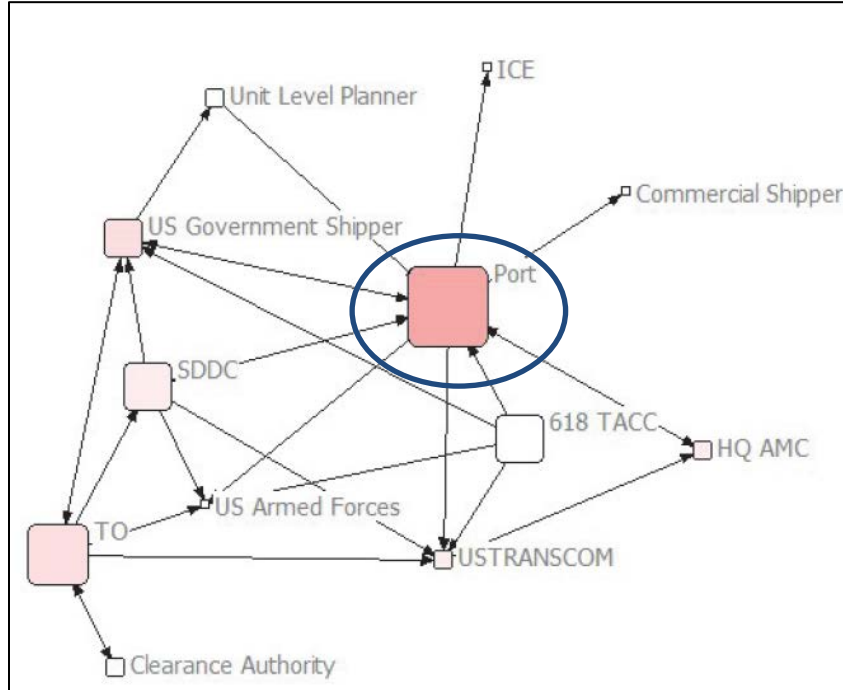
analytical perspective of the cyber threats specific to AMC, in particularly their logistics systems.

To learn about of the challenges at the tactical level, interviews were conducted at strategic aerial ports based at CONUS and overseas locations. The interviews were comprised of three open-ended questions designed analyze current TTPs and standing operating procedures (SOPs) to mitigate any disruption of GATES during combat operations; the impact such a disruption will have on the facility's ability to effectively conduct its mission; and an understanding of measures to gauge the effectiveness of any mitigation strategies. The three questions were: 1) Are GATES operators (non-cyber personnel) trained to recognize a cyber-attack on the system? 2) What procedures are in place to mitigate attacks on GATES? 3) How many people and man-hours does it require to operate in an environment absent of GATES?

In 2013, the RAND Corporation conducted a study on the impact of a cyber network attack (CNA) on AMC IT logistics systems. The study highlighted how a successful attack on one system can have a devastating impact on the entire IT logistic enterprise due to the interoperability of the systems in the enterprise. Figure 4 shows how the IT logistics systems are interconnected. The decision to make GATES the focus of this research was based on the preponderance of systems that are interfaced with GATES. The same methodology was used when determining which organization at the tactical level would be better suited to provide an in depth analysis the impact a degraded GATES would have on its daily operations. Figure 5 shows the preponderance of GATES activity originates or is exchanged at AMC aerial ports located around the world, very much acting as a hub for GATES information.



**Figure 5: System Network: Information Exchanges Between Logistics IT Systems**  
(RAND 2013)



**Figure 6: Process Owner Network: Information Exchanges Between Process Owners**  
(RAND, 2013)



## IV. Analysis and Findings

### *Data Analysis*

Data was evaluated using the comparative method and was limited to unclassified sources. Input from the aforementioned organizations and government literature contributed to the development of the recommendations.

Table 2 highlights the focus on logistics systems by command level based on the interview questions provided for this research.

**Table 2: Focus of Cyber Logistics Systems by command level**

Interview Questions	Strategic	Operational	Tactical
Are there any Air Force policies and guidelines for safeguarding logistics IT systems when operating in cyberspace?		X	
Are cyber warfare officers and NCO's approach to training focused to defend logistics systems?			
How does the Air Force plan to prepare its logistics forces to work in a cyber contested environment?		X	
What guidelines are given logistics units to defend their systems against a cyber attack?			
What is the most probable form of attack against a GATES?		X	
Are other military services, government agencies and contractors that utilize GATES held to the same security protocols as Air Force systems on the AFNET?		X	
Are GATES operators (non-cyber personnel) trained to recognize a cyber attack on the system?	X	X	
What procedures are in place to mitigate an attack on GATES		X	
How many people and man-hours does it require to operate in an environment absent of GATES?			X

### *Findings*

Table 2 shows the preponderance of the responses to the questions at that the operational level of command focus on logistics systems more than the strategic and tactical levels of command. Although the strategic level of command is responsible for developing policy for all

systems on the AFNET, the focus lies on systems directly tied to combat operations or systems handling information that is determined to be vital to operational readiness.

The operational level of command is charged with identifying system threats as well as developing tactics to mitigate or defend against known threats and when necessary, develop tactics to conduct attacks on adversarial targets. Additionally, the operational level of command expands the focus to include a few logistics systems that are deemed important for the support of deployed and contingency forces.

Based on the responses from the interviews, logistics units at the tactical level (e.g. aerial ports) do not show a focus on a cyber threat to GATES or any other logistics system. In fact, when participants were asked of the actions they will take upon discovering the system had been compromised due to a cyber-attack, they admitted such a scenario has never been exercised. The participants further explained that the same manual procedures that are currently in place in AMCI 24-101 VOL 9 and local SOPs will be exercised in the event of any interruption of GATES.

The following are findings based on the response to questions presented to organizations at the strategic level (SL), operational level (OL) and tactical level (TL) of command.

SL Question 1: *Are there any Air Force policies and guidelines for safeguarding logistics IT systems when operating in cyberspace?* The response was that the Air Force as well as all of DoD has accepted cyberspace as a warfighting domain much like land, maritime, air and space. Much like the physical domains, it is unique in its own right and requires specialized doctrine, police and approaches. Another way in which cyber is similar to the other domains can be a supporting domain or enabler; it enables the other domains by enhancing supporting facets such as logistics, thus making it a force multiplier. As such, from a strategic level, under the

direction and guidance of U.S. Cyber Command (USCYBERCOM), USAF HQ A3/6 work to set policy and doctrine that will incorporate cyber into plans as the legacy domains. The activation of a numbered AF and an Operational Center whose mission is dedicated to cyber related activities is evidence of the breadth of scope cyber has evolved to.

SL Question 2: *Are cyber warfare officers' and NCO's approaches to training focused to defend logistics systems?* The Air Force has made great strides during the past five years in developing cyber warfare specialties with the establishment of the 17D officer as well as the 1B4 enlisted Air Force specialties. However, these specialties serve only as the first generation of what must inevitably become a much more diverse field of professionals with a weapons school dedicated to developing tomorrow's cyber warriors in advanced tactics employment for a particular weapon system (e.g. logistics IT systems).

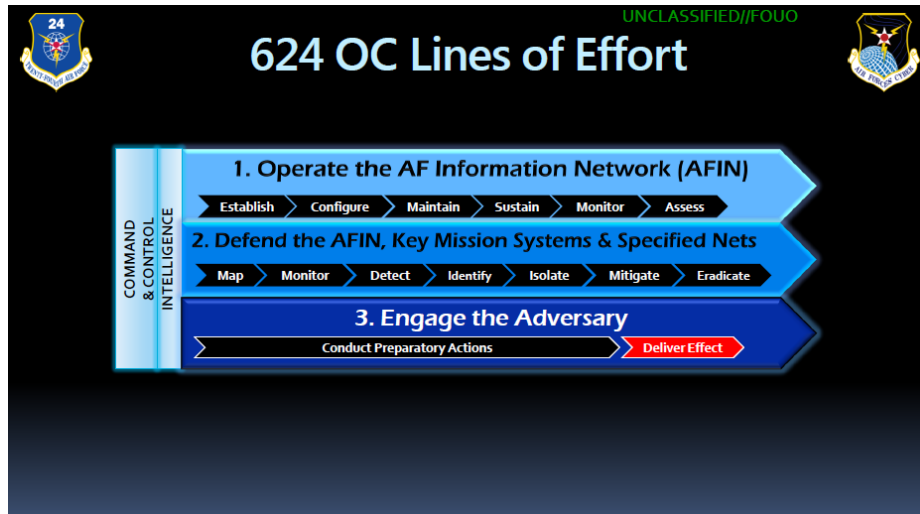
SL Question 3: *How does the Air Force plan to prepare logistics forces to work in a cyber contested environment?* CYBERCOM's premier exercise, Cyber Flag is a full spectrum exercise that provides offensive and defensive training to cyber forces in a closed network environment. Its priorities are: to exercise joint and coalition cyberspace operations and to fully integrate in combatant air, land and sea operations; identify, prioritize and defend "key" cyber terrain against imminent or known threats; operate in a denied, manipulated or contested environment; rehearse command and control of cyberspace forces at the tactical and operations levels. The ultimate goal of the exercise is to operationalize and integrate cyber operations fully into traditional military planning and operations. Currently, Logistic systems are not a focus of Cyber Flag. There are plans to incorporate logistics into future scenarios.

Turbo Challenge is a USTRANSCOM sponsored exercise that tests the Defense Transportation System to support the deployment and sustainment of forces to the Korean

peninsula. Turbo Challenge is a joint U.S.-Korean command post exercise which focuses on Reception, Staging, Onward Movement and Integration (RSOI), which involves electronic communication and coordination of the actual movement of ships and cargoes. However, the exercise does not incorporate GATES into the exercise, which will be a vital system for providing ITV to the commander of the United States Forces Korea.

OL Question 1: *What guidelines are given logistics units to defend their systems against a cyber-attack?* The 24th Air Force was developed to become the Air Force's warfighting organization that executes full spectrum cyberspace operations. Within the 24th Air Force organization is the 624th Operations Center (624 OC), which functions as a traditional Air Operations Center (AOC), only instead of tasking wings, it tasks functional units; produces a cyber tasking order (CTO) instead of an air tasking order (ATO) that is used to task and execute assigned and attached cyber forces in support of CDRUSCYBERCOM and theater JFC's objectives (624th OC, 2014).

The 624 OC was developed to provide an entity capable of providing the means to develop strategy, organize cyberspace forces, task, and control them to achieve operational effects across the cyberspace domain that are integrated with the other warfighting domains. Figure 6 shows the 624 OC's lines of effort, which provides commanders a visualization of its military capabilities.



**Figure 7: 624 OC Lines of Effort (624th OC, 2014)**

The 624 OC is part of the Air Force’s shift in paradigm in its approach to cyber operations, in particular the defense of its systems. The previous approach to cyber threats was to protect everything under the enclave equally. This approach was neither efficient nor effective. Today, the Air Force developed the concept of defense in depth, which implements multiple protection measures in series in order to avoid a single point of failure. This enables the 624 OC to operate, defend and engage on only select systems that are believed to be vital to mission accomplishment.

Department of Defense Instruction (DODI, 8580.1) sets the guidelines that define the Mission Assurance Category (MAC) levels placed on systems based on “the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission.”

The DoD has three MAC levels. MAC I is reserved for the systems considered most detrimental to the war effort (there are no logistics systems in MAC I); MAC II are those systems deemed “important” to the support of deployed forces, which is the level GATES is protected under and is defined as follows:

*Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.*

MAC III systems are the systems with the lowest safeguards.

OL Question 2: *What is the most probable form of attack against GATES?* Based on open source information, a clever adversary will probably not conduct a direct attack on GATES. In fact, the attack may go on unnoticed like the Stuxnet attack for a significant amount of time. The attacker may snoop around the system to learn more about its procedures. A method that is popular among the cleverest attackers is indirectly attacking the system through a more vulnerable area or a softer target such as a SCADA system or an unsuspecting member. The point of attack may occur through a user's wireless or Bluetooth device that has access to the Air Force Network (AFNET). This surreptitious attack does not require the target to be physically on the installation or commercial partner facility. There are other forms of attacks that GATES is susceptible to that require a high level of expertise that is normally only found by attacks conducted or sponsored by nations that is outside the classification of this research.

OL Question 3: *Are other military services, government agencies and contractors that utilize GATES held to the same security protocols as Air Force systems on the AFNET?* The DoD Information System Certification and Accreditation Reciprocity states that if one service's IT system is accredited and certified within the DoD Information Assurance Certification and Accreditation Process (DIACAP), the other services should have the confidence to place that

system on their service network. This process allow for accreditations and the ability to connect to non-homogenous systems. GATES is a prime example of a system that is reliant on the Reciprocity process. This methodology is inherently risky since an agency to oversee the program does not exist to enforce the security controls put in place or the ongoing effort to keep systems secure.

The process is deigned that if a service has an enterprise level system (e.g., GATES) and the DoD Information Security Risk Management Committee (ISRMC) grants the service an accreditation it should be accepted across all services, thus establishing transparency and trust in a standard level of security. Some services have been reluctant to comply with the mandate, yet continue to use GATES as a necessity to move their cargo. Transparency and cross referencing of IT security systems with other services is vital for the integrity of the entire network enterprise. Not being aware of the network capability of other services adds risk to systems such as GATES that are reliant on the unknown capability of other services and agencies that may have less stringent or incompatible protocols.

TL Question 1: Are GATES operators (non-cyber personnel) trained to recognize a cyber-attack on the system? What is the impact to the mission in the event GATES is compromised? Interviews were conducted at strategic aerial ports based in CONUS and overseas. The response from the questionnaire proved to be consistent with the results of the interviews with some variances due to the size and mission of the aerial port. AMCI 24-101 series provides guidance on aerial port procedures from which many of the units' SOPs are derived.

Green Sheets and Purple Sheets enable the CCDR the flexibility to prioritize cargo she deems necessary for the AOR or for national security. An environment absent of GATES requires the load planning section to physically ensure the statement "Purple Sheet" as of (in the

clear date and time of request) is typed or printed in the remarks block (item 21) of the DD Form 1384, Transportation Control Movement Document (TCMD) manually, leaving more room for error during high-stress periods.

The PHOENIX RAVEN teams are specially trained security forces personnel with the responsibility of guarding AMC aircraft in high-threat areas. When unable to coordinate movement of PHOENIX RAVEN teams with 618 AOC (TACC)/XOGC within 24 hours when flying on passenger bookable channel missions, HQ AMC/A7S must coordinate with the AMC passenger terminal activity that the PHOENIX RAVEN team is scheduled to depart from. The AMC passenger terminals must then port-book the team members at the terminal of departure to ensure transportation for the team (Air Mobility Command, 2014). With a fully operational GATES, this process is normally transparent and seamless. The absence of the autonomous capability that GATES provides makes it more cumbersome and vulnerable to human error.

TL Question 2: What procedures are in place to mitigate attacks on GATES? Every aerial port that responded to the survey regardless of the size of its mission responded that their unit had manual procedures identified in their SOPs based on AMCI 24-101, Vol. 9 and other volumes to process cargo and personnel. It must be noted that none of the participating units considered the cause of GATES being down or inoperative as a result of a cyber-attack. This lack of awareness may be detrimental to the defense-in-depth efforts of the 624 OC, where information from the end user is a critical component of that architecture.

The larger strategic aerial ports are mostly equipped with the advanced mechanized material handling system (MMHS). This automated system is comprised of conveyor belts, scales, highline docks and omni-roller boards and is interfaced with GATES to automatically capture



and input accurate weight, dimensions and location of the cargo in the facility for expedient movement for shipping.

During a large troop movement, passengers move through a number of AMC aerial ports. GATES is designed to update the manifest information in IGC and provides inbound passenger manifest data to the aerial port of debarkation (APOD) and other receiving activities for planning and Joint Reception and Onward Integration (JRSOI) management activities. Upon passengers' arrival at the APOD, information about their onward movement will be passed to IGC. In an environment absent of GATES, the port must use DD Form 2131, Passenger manifest to capture all the vital data in accordance with (IAW) DOD 4500.9R, Defense Travel Regulation (DTR) Part I, Passenger Movement in order to coordinate sufficient airlift assets and meet ITV requirements.

TL Question 3: How many people and man-hours does it require to operate in an environment absent of GATES? A disruption of GATES will require the entire process to be done manually, which the interviewees and questionnaire participants responded it would take an additional 45 minutes to 90 minutes to process and load the cargo. In particular for processing cargo originating at the port where the incidence occurred because it is prior to cargo aggregation.

Current manning calculations for the aerial ports are based on the time it takes to process cargo with the MMHS being fully operational. Based on the current manning, if GATES capability is compromised or degraded, the aerial ports will quickly exceed their mission capability causing a domino effect to other receiving activities along the supply chain. This loss in capability will certainly be a significant blow to air power projection during surge operations.

## V. Conclusions and Recommendations

### *Conclusions of Research*

Breaking down requirements into functional and technology classes may help to more clearly articulate cyber warfare disconnects within the program objective memorandum (POM) process. Additionally, it can assist the CDR's planners in requesting appropriate cyber warfare forces from the Air Force and enable the Air Force to better train its cyber force to meet the CDR's needs. A logical system for categorizing groups of technologies and functions within cyberspace does not formally exist today. However, we will need one if we wish to organize, train, and resource cyber warfare capabilities effectively in the future.

The U.S. Air Force Weapons Course (USAFWC) exists to provide deployed forces a weapons officer capable of integrating the entire spectrum of Air Force capabilities to conduct integrated combat operations. A weapons officer that specializes in the capability of logistic systems will better serve a joint forces commander by providing the commander a deeper understanding of the unique capabilities and vulnerabilities of the system(s).

GATES is an integral part of the DoD IT infrastructure that enables warfighters to operate more efficiently in today's modern warfare. It has a prominent role in the employment of the Rapid Global Mobility and C2 enduring missions of the Air Force. AMC's development of the CTWG is evidence of the command's response to the growing threat on logistic systems that operate in the cyber domain. The system's heavy reliance on unclassified networks not only makes GATES vulnerable to cyber-attacks, but the entire logistics enterprise vulnerable.

The operational level of command has spearheaded a comprehensive communication campaign on the dangers Social networking sites (SNS) such as Facebook, Skype, Twitter and YouTube are to the AFNET. The recent attack on CENTCOM's SNS site is evident of this.

However, there is no evidence that GATES users are warned of how those vulnerabilities may have similar repercussions on GATES and the entire logistics enterprise. The air Force information awareness campaign has raised awareness about the vulnerability Air force systems exposed to systems outside the AFIN. A more robust I.A. program with an emphasis on cyber and GATES as a weapon system directed to all its users may raise awareness, thus minimize the threat.

### ***Recommendations for Future Research***

DoD and the Air Force must treat the cyber domain as the physical domains: land, maritime, air and space. The sooner it is acknowledged and accepted, training in cyber as training the other domains, non-cyber forces will be better equipped to minimize the risk involved in working in that domain, thus becoming a force multiplier. Just as traditional forces secure lines of communication in the terrestrial domains to exploit an adversary's capabilities, so should protocols exist that secure the cyberspace architecture in order to employ systems without fear of interruption or denial of service. Much like the infantry is the foundation to a ground war; DoD must incorporate the same culture for the cyber domain.

Future research must continue to explore how to better incorporate logistics IT systems in major exercises. Red Flags or Air Force Weapon School exercises, employ such a mechanism in the form of a "threat replication" matrix to identify the level of sophistication in order to train blue forces to employ various levels of TTP levels for offensive cyber warfare capabilities range from the least sophisticated, to more advanced techniques, such as: active deception, highly cloaked anonymous operations, etc., which are capable of producing second and third-order effects. These exercises build operational rigor into war-fighting forces; however, there lacks a robust scenario providing a significant threat to logistic IT systems over the cyber domain. To

echo the 2013 study by RAND Corporation, DoD and Air Force level exercises such as Cyber Flag and Turbo Challenge must include a realistic cyber threat scenario against a logistics system for cyber and non-cyber personnel in order to develop TTPs and heighten awareness.

There needs to be more coordination during system implementation and development of IT systems and applications that supports them. Currently penetration tests are conducted after a system has been implemented. Conducting these tests during this time versus during the development phase significantly increases the overall cost of the program. None can be done without Senior Leader involvement. The cost savings may afford the necessary funds to move GATES to a MAC I level of support.

As explained by Zimmerman, Norris and Fraser in their 2014 Joint Staff College paper, “Countering Atlantis: The Cyber Threat to Critical Infrastructure that Supports Logistics”, the DoD needs to develop a more robust cyber understanding at the field grade level to more effectively integrate cyber into exercises, plans, and operations. Zimmerman, et al. recommended the implementing cyber capabilities and limitations education for field grade officers by integrating into the Joint Professional Military Education.


Further study should be conducted to determine if more education on cyber threats and vulnerabilities should be implemented into every aspect of professional military education for the officers and enlisted corps. Based on the interviews, members at the strategic and operational levels of command displayed a sound understanding of the threats and vulnerabilities of IT systems operating on the cyber domain. Due to the information campaign provided by the 624 OC, members at the tactical are aware of cyber vulnerabilities on the AFNET, but do not seem aware of how it may impact GATES or any other logistics systems operating on the AFNET.

Implementing cyber education in all PME curricula may aid in meeting the intended integration of cyber into all facets of military planning and C2 process.


There are a number of checks and balances between various sections at the aerial ports (e.g., ATOC and load planning) to ensure the integrity of the cargo before it departs the station. Unfortunately, an environment absent of GATES challenges these professional transporters with accurately documenting the weights, dimensions and air commodity codes (critical for separating hazardous cargo) expeditiously during a surge. Currently each aerial port has its own procedures on how to conduct manual operations when GATES is inoperable. Establishing standardized stand-alone automated procedures will provide the capability to seamlessly continue operations during a surge with limited disruption to the operation.

Interviews were conducted at strategic aerial ports based in CONUS and overseas. The response from the questionnaire proved to be consistent with the results of the interviews with some variances due to the size and mission of the aerial port. The consistency may be attributed to the guidance set forth in AMCI 24-101 series which give guidance on aerial port procedures from which many of the units' SOPs are derived.

# Appendix



## Fighting Through a Logistics Cyber War



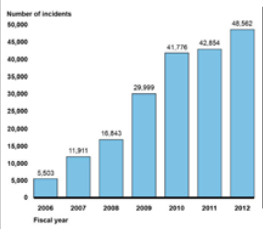
### Introduction

Cyber-attacks on information systems in the United States have steadily increased over the past decade. The true magnitude of these attacks was not revealed to the public until 2013, the White House authorized the Federal Bureau of Investigation to notify over 3,000 companies in the private sector that their computer systems and networks had been compromised. These attacks are carried out by various types of criminal factions and foreign governments. The White House has directly accused China of orchestrating deliberate attacks on American government systems, to include defense contractors.

A cyber-attack on DoD Information systems could severely degrade or disrupt the ability of the United States military to rapidly and effectively project decisive power against adversaries. The logistics enterprise is particularly vulnerable, given the scale of operations required to support the war fighter and its heavy reliance on unclassified networks.

This research focuses on The Global Air Transportation Execution System (GATES), managed by Air Mobility Command (AMC), which supports worldwide DoD transportation needs in peace and war by managing cargo and passenger information transiting through AMC aerial ports around the world. A cyber-attack on GATES could potentially degrade the force projection capability needed to meet operational requirements. This study aims to...

### Maj Anthony Mollison Advisor: Jeffrey A. Ogden, PhD Advanced Studies of Air Mobility (ENS) Air Force Institute of Technology



Year	Number of Incidents
2006	5,533
2007	11,911
2008	16,843
2009	29,999
2010	41,716
2011	42,854
2012	48,562

### Methodology

This study supplements previous and existing projects aimed at improving the defense of USTC and AMC logistics systems that are heavily reliant on the dot com domain to conduct their mission. In an effort to get a full understanding of the impact of cyber-attacks on Air Force logistics systems, interviews were conducted with cyber and GATES experts at the strategic, operational and tactical levels of command.

In order to better understand Air Force strategic cyber policies and command structure, interviews were conducted with members of U.S. Air Force Headquarters, A3W (USAF HQ A3W). Additionally, USAF HQ A3W detailed U.S. Air Force's role in the Comprehensive National Cybersecurity Incentive (CNICI) efforts to defend the U.S. information and communications infrastructure.

This research only examined the unclassified vulnerabilities of GATES that can be referenced back to open sources. To better understand the challenges of working in cyberspace and the operational vulnerabilities Air Force members must overcome while conducting their daily activities, interviews were conducted with cyber experts from the 24th Air Force and 624th Operations Center.

### Research Goals


This project will focus on The Global Air Transportation Execution System (GATES), managed by Air Mobility Command (AMC), which supports worldwide DoD transportation needs by managing cargo and passenger information transiting through AMC aerial ports around the world. A cyber-attack on GATES could potentially degrade the force projection capability needed to meet operational objectives. This study will show how such an attack on GATES could potentially degrade the Air Force's ability to establish and sustain expeditionary base operations and meet sortie generation requirements. This study will also investigate the policies in place that provides guidance for the strategies and TTPs that counter and mitigate such attacks on GATES.

Interview Questions	Strategic	Operational	Tactical
Are there any Air Force policies and guidelines for safeguarding logistics IT systems when operating in cyberspace?	X		
Are cyber warfare officers and NCO's approach to training focused to defend logistics systems?		X	
How does the Air Force plan to prepare its logistics forces to work in a cyber contested environment?		X	
What guidelines are given logistics units to defend their systems against a cyber attack?			
What is the most probable form of attack against a GATES?		X	
Are other military services, government agencies and contractors that utilize GATES held to the same security protocols as Air Force systems on the AFNET?		X	
Are GATES operators (non-cyber personnel) trained to recognize a cyber attack on the system?	X	X	
What procedures are in place to mitigate an attack on GATES		X	
How many people and man hours does it require to operate in an environment absent of GATES?			X

### Focus of Cyber Logistics Systems by command level

### Collaboration

HQ USAF/ A6, 24AF, 624th OC, HQ AMC/A4



AIR FORCE INSTITUTE OF TECHNOLOGY

## VI. Bibliography

- 2600 News. (2000, March 2). *Mitnick to Testify Before the Senate Committee*. Retrieved from 2600 News: <http://www.2600.com/news/view/article/334>
- 624th OC. (2014, August 20). *624th OC Perspective*. Retrieved from [http://c.ymcdn.com/sites/www.alamoafcea.org/resource/resmgr/files/\(u\)\\_624\\_oc\\_afcea\\_presentation.pdf](http://c.ymcdn.com/sites/www.alamoafcea.org/resource/resmgr/files/(u)_624_oc_afcea_presentation.pdf)
- 624th OC. (2014, October 27). Bluetooth Faces Perception of Vulnerability: Bluejacking, Bluesnarfing and Bluebugging. *Cyber Threat Bulletin*.
- Abbate, J. (1999). *Inventing The Internet*. Cambridge: The MIT Press.
- Ackerman, R. K. (2008, April). *Future Threats Drive U.S. Intelligence* . Retrieved from Signal: <http://www.afcea.org/content/?q=future-threats-drive-us-intelligence>
- Air Mobility Command. (2012, December 31). *Air Transportation Requirements*. Retrieved from air Force ePublishing: <http://www.e-publishing.af.mil/>
- Air Mobility Command. (2014, February 20). *AIR TERMINAL OPERATIONS CENTER*. Retrieved from Air Force e-Publishing: <http://www.e-publishing.af.mil/>
- Anthony Rosello, E. B.-B. (2013). *What Is the Impact of a Cyber Attack on Air Mobility Command's Logistics Information Technology Systems and Processes?* Pittsburgh: RAND.
- Atomic Bomb Museum. (2006). *Destructive Effects*. Retrieved from AtomicBombMuseum.org: [http://atomicbombmuseum.org/3\\_radioactivity.shtml](http://atomicbombmuseum.org/3_radioactivity.shtml)
- Basla, M. (2013). *Air Force Information Dominance Strategy*. Washington DC: USAF. Retrieved from <http://www.safcioa6.af.mil/shared/media/document/AFD-141006-038.pdf>
- Buley, T. (2008, November 20). *Hacking Airport Wi-Fi*. Retrieved from Forbes: <http://www.forbes.com/forbes/2008/1208/052.html>
- Castrodale, J. (2015, March 28). *Security Vulnerability In Hotel Wifi Could Allow Hackers to Access Guests Computers, Personal Info*. Retrieved from USA Today: <http://roadwarriorvoices.com/2015/03/28/security-vulnerability-in-hotel-wi-fi-could-allow-hackers-to-access-guests-computers-personal-info/>
- Chi, M. (2014, November 14). *Cyberspace: America's New Battleground*. Retrieved from SANS Institute: <http://www.sans.org/reading-room/whitepapers/warfare/cyberspace-americas-battleground-35612>

- Clausewitz, C. V. (1989). *On War*. Princeton: Princeton University Press.
- Constantin, L. (2013, December 10). *Hackers said to infiltrate European foreign affairs ministries ahead of G20*. Retrieved from PC World:  
<http://www.pcworld.com/article/2071540/hackers-said-to-infiltrate-european-foreign-affairs-ministries-ahead-of-g20.html>
- Cook, J. (2014, October 6). *FBI Director: China Has Hacked Every Big US Company*. Retrieved from Business Insider: <http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10>
- Department of Homeland Security. (2013, November 1). *Cybersecurity Overview*. Retrieved from Department of Homeland Security: <http://www.dhs.gov/cybersecurity-overview>
- Finkle, J. (2013, February 26). *Researchers say Stuxnet was deployed against Iran in 2007*. Retrieved from Reuters: <http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226>
- Fire Eye Inc. (2013). *The Advanced Cyber Attack Landscape*. Retrieved from Fire Eye:  
<http://www.security-finder.ch/fileadmin/dateien/pdf/studien-berichte/fireeye-advanced-cyber-attack-landscape-report.pdf>
- Franz, T. (2011). The Cyber Warfare Professional: Realizations for Developing the Next Generations. *Air & Space Power Journal*, 25(2), pp. 87-99.
- Gregory Korte, K. J. (2014, December 18). *Authorities Increasingly Satisfied N. Korea Behind Hack*. Retrieved from USA Today:  
<http://www.usatoday.com/story/news/politics/2014/12/18/sony-north-korea-hack-department-of-justice-fbi/20584367/>
- Griffiths, R. T. (2002). *From ARPANET to the World Wide Web*. Retrieved from Universiteit Leiden: History of the Internet, Internet for Historians:  
[http://www.let.leidenuniv.nl/history/ivh/frame\\_theorie.html](http://www.let.leidenuniv.nl/history/ivh/frame_theorie.html)
- Grossman, D. (2015). *The Evolution of Weaponry*. Retrieved from Killology.com:  
<http://www.killology.com/Weaponry.htm>
- Joint Chiefs of Staff. (2011, August 11). *Joint Publication 5-0: Joint Operation Planning*. Retrieved from Air Force ePublishing:  
[http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_17.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf)
- Joint Chiefs of Staff. (2013, June 6). *Joint Publication 4-01: The Defense Transportation System*. Retrieved from Air Force ePublishing: <http://www.e-publishing.af.mil/>



- Joint Chiefs of Staff. (2014). *Joint Pub 3-13: Information Operations*. Washington D.C.: Department of Defense.
- (2009). *Joint Publication 3-17 Air Mobility Operations*. Department of Defense.
- Lamothe, D. (2015, January 12). *U.S. Military Social Media Accounts Apparently Hacked by Islamic State Sympathizers*. Retrieved from The Washington Post: <http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/>
- Lenkart, J. J. (2011). *The Vulnerability of Social Networking Media and The Insider Threat: New Eyes for Bad Guys*. Monterey: Naval Post Graduate School.
- Lin, S. E. (2007). *Toward a Safer and More Secure Cyberspace*. Washington D.C. : National Academy of Sciences.
- Lisko, T. (2010, September 6). *The Robin Sage Experiment: Interview with Omachonu Ogali*. Retrieved from Privacy Wonk: <http://www.privacywonk.net/2010/09/the-robin-sage-experiment-interview-with-ogali-om.php>
- Massoud, S. A. (2010). *Spring Issue of the Bridge on the Electricity Grid*. Retrieved from National Academy of Engineering: <https://www.nae.edu/Publications/Bridge/TheElectricityGrid/18868.aspx>
- McGuinness, T. (2011). *Defence in Depth*. Retrieved from SANS Institute InfoSec Reading Room: <http://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525>
- Menon, S. (2014, November 29). *Our Dependence on Cyberspace*. Retrieved from Business Standard: [http://www.business-standard.com/article/opinion/our-dependence-upon-cyberspace-113071300661\\_1.html](http://www.business-standard.com/article/opinion/our-dependence-upon-cyberspace-113071300661_1.html)
- Moskowitz, R. (2002, October 11). *The Myth Of Hiding SSIDs*. Retrieved from TISC Insight Newsletter: <http://tisc-insight.com/>
- Nakashima, E. (2014, March 24). *U.S. notified 3,000 companies in 2013 about cyberattacks*. Retrieved from The Washington Post: [http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9\\_story.html](http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html)
- Nasr, S. L. (2015, February 13). *Top 10 Game-changing Military Technologies*. Retrieved from How Stuff Works: <http://science.howstuffworks.com/10-game-changing-technologies.htm#page=1>

- Office of Management and Budget. (2008). *Circular No. A-11: Preparation, Submission and Execution of the Budget*. Retrieved from White House: [http://www.whitehouse.gov/sites/default/files/omb/assets/a11\\_current\\_year/a\\_11\\_2008.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2008.pdf)
- Piggin, R. (2010). The Reality of Cyber Terrorism. *Engineering and Technology*, 36 -38.
- PWC. (2014, September 30). *The Global State of Information Security*. Retrieved from PWC: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/>
- Rietscha, E. (2012). *Lightweight Portable Security (LPS)*. Retrieved from Military CAC: <https://militarycac.com/PDFs/LPSInfo.pdf>
- Sanchez, R. (2014, February 24). *US to cut army size to pre-Second World War levels*. Retrieved from The Telegraph: <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10658970/US-to-cut-army-size-to-pre-Second-World-War-levels.html>
- Sanger, D. E. (2013, May 6). *U.S. Blames China's Military Directly for Cyberattacks*. Retrieved from The New York Times: [http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=0)
- Stark, H. (2011, August 8). *Spiegel Online International*. Retrieved from Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War: <http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html>
- Statista. (2015). *Victim countries most affected by cyber espionage in 2013, by share of incidents*. Retrieved from Statista: <http://www.statista.com/statistics/330286/cyber-espionage-selected-victim-countries/>
- Stokholm International Peace Research Institute. (2014, April). *Recent Trends in Military Expenditure*. Retrieved from SIPRI: <http://www.sipri.org/research/armaments/milex/recent-trends>
- Symantec. (2011, September 7). *Norton Study Calculates Cost of Global Cybercrime: \$114 Billion Annually*. Retrieved from Symantec: [http://www.symantec.com/about/news/release/article.jsp?prid=20110907\\_02](http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02)
- U.S. Senate, Committee on Armed Services. (2014, December 2). *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*. Retrieved from [http://www.armed-services.senate.gov/imo/media/doc/SASC\\_Cyberreport\\_091714.pdf](http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf)
- United Nations. (2011, December 12). *Cybersecurity: A global issue demanding a global approach*. Retrieved from United Nations Department of Economic and Social Affairs:

<http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>

United States Government Accountability Office. (2013). *Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address the Persistent Challenges*.

Washington D.C.: United States Government Accountability Office.

Williams, B. T. (2011). Ten Propositions Regarding Cyberspace Operations. *Joint Force Quarterly*, 10-17.

Zetter, K. (2012, May 28). Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. Retrieved from Wired: <http://www.wired.com/2012/05/flame/all/>

Zimmerman, C. F., Norris, V., & Frasier-Loria, J. (2014). *Countering Atlantis: The Cyber Threat to Critical Infrastructure that Supports Logistics*. Norfolk: Joint Forces Staff College.

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved</i> <i>OMB No. 0704-0188</i>		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 06-19-2015		2. REPORT TYPE GRP		3. DATES COVERED (From — To) May 2014 - Jun 2015	
4. TITLE AND SUBTITLE  Fighting Through a Logistics Cyber Attack			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)  Mollison, Anthony R., Major, USAF			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology, Graduate School of Engineering and Management (AFIT/EN), 2950 Hobson Way WPAFB, OH 45433-7765			8. PERFORMING ORGANIZATION REPORT NUMBER AFIT-ENS-GRP-15-J-027		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) United States Air Mobility Command Robert Daniel/AMC/A4 Information Assurance Officer 402 Scott Drive DSN: 779-4649 Scott Air Force Base, IL 62225-5357 daniel.roberts.21civ@us.af.mil			10. SPONSOR/MONITOR'S ACRONYM(S) HQ AMC/A4PI		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.					
13. SUPPLEMENTARY NOTES This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.					
14. ABSTRACT Cyber-attacks on information systems in the United States have steadily increased over the past decade. The true magnitude of these attacks was not revealed to the public until in 2013, the White House authorized the Federal Bureau of Investigation to notify over 3,000 companies in the private sector that their computer systems and networks had been compromised. These attacks are carried out by various types of criminal factions and foreign governments. The White House has directly accused China of orchestrating deliberate attacks on American government systems, to include defense contractors. A cyber-attack on DoD information systems could severely degrade or disrupt the ability of the United States military to rapidly and effectively project decisive power against adversaries. The logistics enterprise is particularly vulnerable, given the scale of operations required to support the war fighter and its heavy reliance on unclassified networks. This research focuses on The Global Air Transportation Execution System (GATES), managed by Air Mobility Command (AMC), which supports worldwide DoD transportation needs in peace and war by managing cargo and passenger information transiting through AMC aerial ports around the world. A cyber-attack on GATES could potentially degrade the force projection capability needed to meet operational requirements.					
15. SUBJECT TERMS Cyber, Logistics, GATES					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			UU
U	U	U			19b. TELEPHONE NUMBER (Include Area Code) (937) 255-3636 ext 4653 Jeffrey.Ogden@afit.edu