3-2005

Determining a Relationship between Foreign News Media Reports covering U.S. Military Events and Network Incidents against DOD Networks

Jason D. Jaros

DETERMINING A RELATIONSHIP BETWEEN FOREIGN NEWS MEDIA REPORTS COVERING U.S. MILITARY EVENTS AND NETWORK INCIDENTS AGAINST DOD NETWORKS

THESIS

Jason D. Jaros, Captain, USAF

AFIT/GIR/ENV/05M-08

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GIR/ENV/05M-08

DETERMINING A RELATIONSHIP BETWEEN FOREIGN NEWS MEDIA REPORTS COVERING U.S. MILITARY EVENTS AND NETWORK INCIDENTS AGAINST DOD NETWORKS

THESIS

Presented to the Faculty

Department of Systems Engineering Management

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 Information Resource Management

Jason D. Jaros, BS

Captain, USAF

March 2005

AFIT/GIR/ENV/05M-08

DETERMINING A RELATIONSHIP BETWEEN FOREIGN NEWS MEDIA REPORTS COVERING U.S. MILITARY EVENTS AND NETWORK INCIDENTS AGAINST DOD NETWORKS

Jason D. Jaros, BS
Captain, USAF

Approved:

/Signed/	15 Mar 05
David D. Bouvin, Capt, USAF, Ph.D. (Chairman)	Date
/Signed/	15 Mar 05
Kevin L. Elder, Ph.D. (Member)	Date
/Signed/	15 Mar 05
Robert F. Mills, Ph.D. (Member)	Date

Abstract

This thesis explores the nature of the relationship between foreign news media and network incidents against DoD networks. A rank correlation was performed between the number of network incidents against DoD networks and foreign news media reports covering U.S. Military events. Further analysis was conducted to determine the key terms used in the contents of foreign news media reports for the months the reports were significantly correlated with network incidents. Several significant correlations were found between various combinations of regions and categories of network incidents. However, the correlations were only moderate and the key terms only led to a slightly better understanding of such relationships.

Acknowledgments

I would like to first express my sincere appreciation to all my committee members whose advice has made this thesis a better product. I would specifically thank my advisor, Capt Dave Bouvin, whose unwavering support was a major motivation for my efforts. I would also like to thank Captain Alex Svetlev and the organization he worked for, NetDefense as well as Foreign Broadcast Information Systems who provided the data without which this thesis would not have been possible. Finally I thank my family for all the laughs when times were busy and stressful and the distractions when I had nothing better to do.

Jason D. Jaros

Table of Contents

Page

Page

List of Figures

Figure Page

List of Tables

DETERMINING A RELATIONSHIP BETWEEN FOREIGN NEWS MEDIA REPORTS COVERING U.S. MILITARY EVENTS AND NETWORK INCIDENTS AGAINST DOD NETWORKS

I. Introduction

Background

Used for storing, processing, or transferring data, information systems are heavily relied upon by U.S. military forces for successful operations, such as aerial attacks, payroll, peace missions, and training. This reliance on information systems is a result of the advantages of real time information acquisition and processing. Information superiority is now a core competency of the U.S. Air Force and a necessary attribute of all military operations. Information superiority is defined in Joint Publication 3-13 (1998) as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. The DoD accomplishes information superiority through the implementation of information operations (IO).

Joint Publication 3-13 (1998) defines IO as actions taken to affect adversary information and information systems while defending one's own information and information systems. Defensive IO guarantees timely, accurate, and relevant information access while denying exploitation of friendly information and information systems through policy and procedures, operations, personnel, and technology. A further subset of defensive IO is information assurance (IA). IA is the protection and defense of

information system availability, integrity, authentication, confidentiality, and non-repudiation.

IA is carried out for the DoD by NetDefense, also known as the DoD Computer Emergency Response Team (CERT). NetDefense assesses incident data collected from the Joint CERT Database (JCD) which is populated by all DoD organizations. An incident is one network attack or several network attacks related to each other through significant similarities in attackers, techniques, victims, and timing (Howard, 1997). A network attack is an unauthorized attempt to access a computer, regardless of whether or not the attempt was successful. Figure 1 illustrates the number of incidents per month against DoD networks for the past two years.

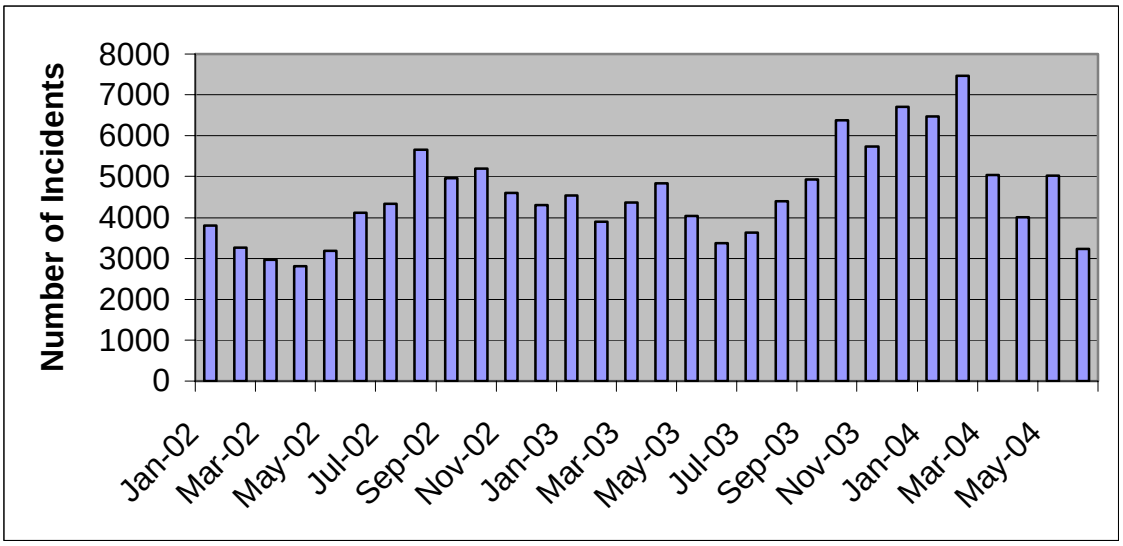

Figure 1: Monthly NetDefense statistics on Incidents Reported from January 2002 though June 2004 (JTF-GNO GNC NetDefense, 2004).

IA is necessary because of the numerous vulnerabilities inherent in information systems. These vulnerabilities include a lack of reliable intrusion detection tools, insufficient security manpower, information system complexity and size, and a

monoculture of tools operating on the information systems (CERT/CC, 2003). Intrusion detection systems (IDS) are unable to analyze all network traffic because data transfer rates are too fast and IDS processing speeds are too slow (Allen, Christie, Fithen, McHugh, Pickel, Stoner, 2000). Furthermore, IDS methods for detecting new types of intrusions are unreliable because the primary detection method compares old intrusion data with current data. The more variation between a new attack and older attacks, the less likely the new attack will be detected. To compensate for the lack of reliability in IDS, manual detection techniques are also used. However, the increasing number of attackers and amount of data to be analyzed is a growing burden for a limited security workforce. The burden on security is further increased because of the size and complexity of information systems (CERT/CC, 2003). Networks include numerous users and multiple connections to the internet along with remote servers; each new component adds to the complexity of the overall system. The complexity is minimized in the DoD by implementing standardized equipment and procedures for each network. The use of similar equipment, however, creates a less complex environment for an adversary to plan an attack against. It is simpler because the attacker would otherwise have to employ separate attack techniques against different types of operating systems, network routing equipment, software applications, etc. Regardless of the employment of IDS tools and improved security procedures, the number of incidents per year has increased steadily for the past several years.

Some of the reasons for the reported increase in incidents may include the use of better intrusion detection tools and practices and increased participation in incident

reporting (CERT/CC, 2003). These factors suggest a greater incident volume unaccounted for in previous years. Increased participation in incident reporting was due to the benefits each contributor gained in understanding attack methods by combining their incident information. This information was used to create better procedures and tools to detect and deny attacks.

Other reasons for the rising number of network incidents are attacker's use of better network attacking tools (Allen, et. al, 2000), the proliferation of the internet, and an increasing number of potential attackers. User friendly software tools simplify the ability for an individual to perform a network attack so minimal knowledge of information systems is needed by the attacker. Figure 2 illustrates the different types of attack tools created from 1980 through 2000 and the relative amount of intruder knowledge required to use these tools (CERT/CC, 2003).

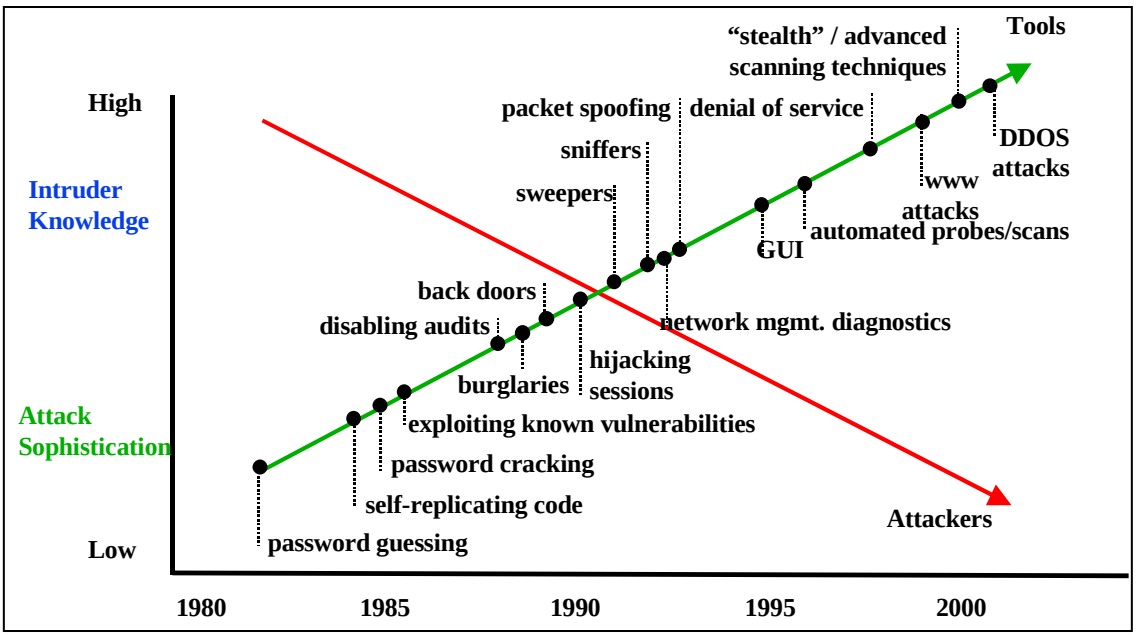

Figure 2: Attack Sophistication vs. Intruder Technical Knowledge (CERT/CC, 2003)

Because it is easy to become an attacker, as more people and organizations connect to the

internet so does the number of potential attackers. Figure 3 shows how the growth of the Internet has increased exponentially for the past decade.

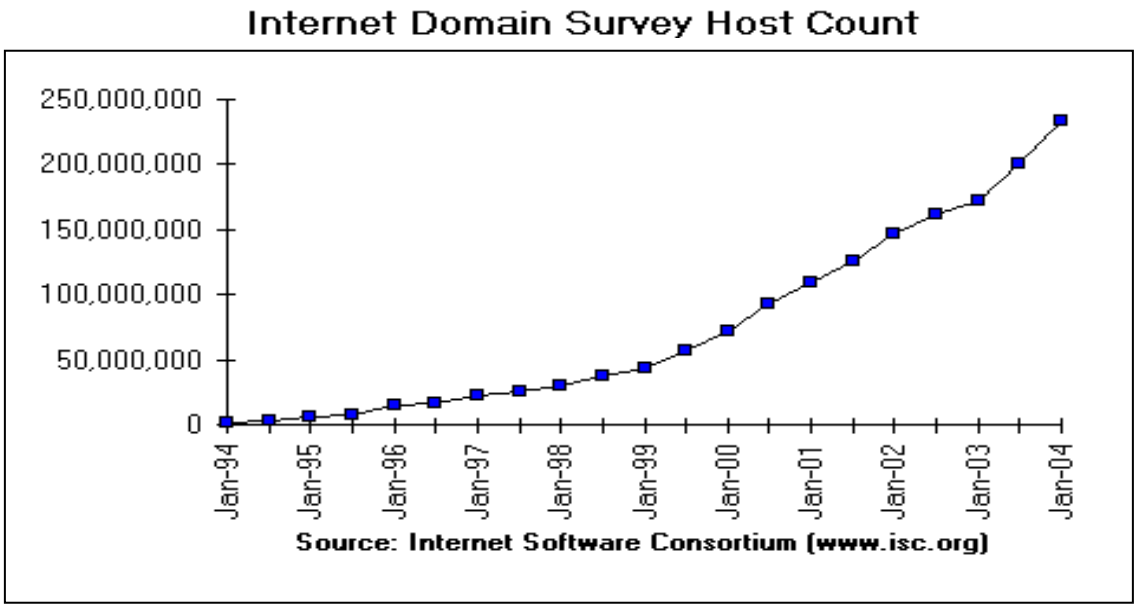

Figure 3: Internet domain survey host count (Source: Internet Systems Consortium, Inc. (http://www.isc.org/))

Several motivations exist for people to conduct network attacks. Howard and Longstaff's (1998) taxonomy clarifies the possible objectives for network attacks as "challenge, status, thrill," "political gain," "financial gain," and "damage." These motivations have been further validated by Diagle (2001). "Challenge, status, thrill" groups three similar motivations together. They are combined because in each case the point of the attack is to do no more then gain access to an information system or bypass its security. An incident is considered "damage" motivated when unauthorized modifications or destruction is done to an information system. Some individuals use their computer skills to gain unauthorized control of an information system and hold it ransom, destroy it, or steal information in hopes of gaining a market advantage. These types of

attacks are done for "financial gain." "Political gain" motivations are similar to financial ones except the results benefit an attacker's government or hinder the victim's government. The public was made aware politically motivated attacks were occurring against the U.S. when in 1998 the CIA director, George Tenet, stated other nation's governments are funding network attacks against the United States (Yurcik, Loomis, and Korzyk, 2000).

The news media has been the public's primary source for information on government actions since the time of the revolutionary war (McHugh, 1997). The information supplied by the news media gives the American public the knowledge of the U.S. government to make necessary decisions or take actions concerning the U.S. government. Therefore, media reports may have a direct influence on the actions of the public (Hill, 1997). Both the U.S. government and its adversaries have taken advantage of the effects the media has on public opinion to gain political advantage (Snyder, 2003). Furthermore, media reports may contain sensitive DoD information which our adversaries could use to their advantage (McHugh, 1997).

DoD public affairs policy has been created to supply the news media with the support it needs for effective reporting and counteract the potential threats created by the news media. Within the policy are guidelines on how to include the media when planning military operations so the public remains well informed, but not give up sensitive information. When the news media gains access to sensitive information it is expected to be secured through self controlled reporting guidelines held by the media (Snyder, 2003). Censorship is still used, but its use is minimized because of the lack of

trust it generates between the government and the public (McHugh, 1997).

It is possible there may be sensitive information being reported not yet known to the DoD. The DoD needs a better understanding of what information should be considered sensitive if this is true. In addition, the number of effects media reports have on public opinion is not fully understood. A better comprehension for the effects media reports have on public actions could lead to improved policy and guidance to reduce negative results.

Problem Statement

DoD officials need to know whether media reports involving military events influence the number of incidents occurring on DoD systems. Network operators need to better prepare DoD information systems against network attacks and DoD officials need better media relationship policies if a relationship is determined to exist. The purpose of this research is to determine what relationships exist between foreign news media coverage of military events and DoD network incidents through qualitative codification and quantitative statistical analysis of data collected by NetDefense and the Foreign Broadcast Information System (FBIS) for the same time period. The hypothesis being tested is whether or not a correlation exists between the frequency of foreign news media reports of military events and the frequency of DoD network incidents. The null hypothesis is that no correlation exists.

Research Questions

What is the nature of the relationship between foreign news media reports covering U.S. military events and network incidents against DoD networks?

Investigative Questions

To better answer the research question, this research proposes to answer the following investigative questions:

1. Do statistically significant correlations exist between different foreign regions of news media reports involving U.S. military events and different categories of DoD network incidents?
2. During what timeframes do the most statistically significant correlations occur?
3. What is the content of the news media reports for the timeframes that are most significantly correlated?

Problem Approach

Data for this research was gathered through the collection of the most recent historical incident data available within the timeframe of this research maintained by NetDefense and a qualitative analysis of eight regions of foreign news media reports maintained by FBIS from January of 2002 to June of 2004. The relationship between each category of incident and news from each foreign region is explored separately to take into account the different possible types of correlations the media may have with DoD network incidents, both positive and negative. The qualitative analysis of media reports was done through the use of a data mining tool, IN-SPIRE. The IN-SPIRE software is used to quantify the number of foreign news media reports containing military events for each day of the study. By using the JMP 5.1 statistical software to perform the Spearman's Rank Test for correlation, the foreign news media and DoD network

incident data were analyzed to determine the existence of any correlations. IN-SPIRE was then used to determine the most significant content of the media reports.

Scope

The point of this research is to find attributes in foreign media reports correlated with network incidents against DoD networks. This research will utilize the most recent daily DoD incident data collected on the JCD attained from NetDefense along with daily foreign media reports acquired from the FBIS for the time period of January 2002 to June 2004. The two and a half year time span will provide a thorough sample of recorded DoD incident data and foreign news media reports. This research does not attempt to suggest what security policy or procedures should be implemented, but investigates the possible correlation between foreign news media reports involving military events and DoD network incidents.

The growing expansion of the internet has made geographical boundaries irrelevant. Because of the internet, network attackers are able to assault any network connected to the internet from virtually anywhere on earth. Therefore, a complete collection of foreign media reports is used for the same time period as the network incident data in this research. Once any significant correlations are found to exist and the content of the news media ascertained, or if no correlations exist, the research will be completed. The practitioner may therefore be able to use the information and determine how the results affect their operations.

Each service, and some individual agencies, maintain a separate network emergency response team to track and repair incidents against their systems. The

incident data from each service is collected on the JCD for further analysis and reporting. For this research the combined data from the JCD attained from NetDefense is used rather than data for each service. One service may have a higher correlation than the other services, but first a correlation should be determined to exist. Data exists for civilian incidents, but it is excluded because this research focuses on information relevant to DoD operations and civilian incident reporting procedures are not as well established as in the DoD.

This research encompasses six of the eight categories of network incidents tracked by the DoD. Of the two categories not employed, incidents classified as "unknown" are excluded because they have yet been properly understood and put into a more meaningful category. Incidents in the category "poor security practice" are also excluded because they are the result of user error. In other words, "poor security practice" incidents are the result of actions not taken to properly secure an information system and fall outside the scope of this research. The remaining six categories (unauthorized access, unauthorized user access, unsuccessful attempted access, denial of service, unauthorized probe, and malicious logic) will be analyzed against the media reports.

Assumptions & Limitations

This research hopes to discover a relationship among DoD network incidents and foreign news media reports covering military events by comparing existing DoD network incident data and foreign media archives. Due to the extremely irregular nature of network incidents, several other factors that affect the number of incidents on DoD

systems could create enough interference to conceal any correlation. As an example, one of the tools used to determine if an incident has occurred, intrusion detection systems (IDS), are far from being a truly accurate measurement device of network incidents (Allen et. al, 2000).

While an abundant number of foreign news media archives exist, it is beyond the abilities and resources of this research to consider every national and international source of media. Rather, this study assumes the over 3000 sources of foreign news media collected and archived by FBIS will be a sufficient sample of foreign news media. The exclusion of media reports from within the United States is assumed not to be a contributing factor to any correlations with other international regions, but may be a consideration for follow-on research.

Because the data are non-parametric, Spearman's Rank test is required to determine a correlation. One potential problem with Spearman's Rank test is when the data have a large number of tied data points relative to the entire data set. When a tie occurs each number is given the same rank based on the amount of numbers with the same value. The result may skew the results of this research. In addition, the values for some of the data sets may fail to reflect a continuous distribution of the two variables being measured. Category I, II, IV incident data and the military related media reports per week data have small values for the samples making this assumption less then ideal. Several more ties may occur as a result. However, the vast accumulation of data within the databases and the large amounts of data for each week seems to satisfy the assumptions required for the Spearman's Rank test. Furthermore, Spearman's test uses

the t-distribution to determine the significance of any correlations. Therefore the validity of a Spearman Rank test depends on a normal distribution of correlation values for the population.

A final limitation is the use of IN-SPIRE to determine the content of media reports. The ability of the IN-SPIRE tool to separate and extract media reports containing U.S. military events from the collection of foreign media is also a potential limitation to this research. Various forms of military operations exist with vague definitions making it difficult to perform a query accurately extract the entire collection of military related news reports. This is especially difficult when the number of news media reports is extremely large, such as the thousands of documents used for this research. Furthermore, while the techniques used to determine the primary content of correlated media reports will be effective and provide valuable insight, they are far from validated with this being the first time IN-SPIRE will be used for research in this manner.

Research Overview

The remaining chapters of this thesis provide the details of this research. Chapter II contains the literature review, which explores the existing body of knowledge pertinent to this research topic. Chapter III describes the method used and assumptions made to analyze the data. Chapter IV provides the findings of the analysis performed on the data. Finally, Chapter V discusses the finding, presents conclusions, and makes recommendations for further research.

II. Literature Review

Chapter Overview

The intent of this chapter is to give the reader a brief review of relevant material concerning the two factors of this research: foreign news media reports covering military events and network incidents against DoD systems. The problem of determining a correlation among the news media's coverage of military events and network incidents is specific yet includes a wide range of topics. Consequentially, only a few research papers exist to use as the basis of this research. The majority of information relating to this research problem consisted of a historical review of network security, the past and present relationship between the news media and the military, DoD network and news media policy, and the effects the media can have on the public.

For the purpose of this thesis the terms “media coverage,” “network incident,” and “military events” need to be clarified. “Media coverage” is any form of publication or broadcast widely distributed throughout a region. Media coverage can therefore take many forms: radio, magazines, newspapers, television, and so forth. The term “network attack” is defined as the unauthorized attempt to view, change, or corrupt information contained on a computer system. A “network intrusion” is a successful attack that results in an attacker having gained access to a network system. A “network incident,” however, is a collection of attacks that share some commonalities, such as a particular victim or goal. Incidents can be distinguished from other incidents because of the sites attacked, techniques used, and individuals performing the attacks. Incidents range from a simple probe of a computer system to the complete destruction of all contents of several

computer networks. Finally, "military events" is defined as any action conducted by the U.S. military.

Computer and Network History

This section presents an overview of relevant history concerning information systems, the Internet, and reasons these systems are vulnerable to network attacks. Within this history it is shown how security and distribution of information are inversely proportionate to one another. This section concludes with a brief review of IDS history and its usefulness as a tracking tool for network attacks.

Information System Technology

Information systems have always proven to be more of an asset then a risk, but as technology has progressed the level of risk compared to the benefits of information systems has increased. Security measures for information systems thirty years ago, such as the mainframe computer, were not as big a concern as they are today. Physical measures were more then capable of handling potential attackers because the information could only be accessed from a single location. Once physical security wasn't sufficient manual auditing became the primary source for ensuring the availability and integrity of information system assets (Witkin, 1995). As the amount of data stored on information systems increased manual auditing became too labor-intensive to be effective. However, the small number of skilled individuals capable of performing a successful attack on information systems minimized the chances an attack would occur on any one system. The advantages of worldwide data communication outweighed the threats of using information systems.

At this point in time security wasn't a large concern. Because of its size the information system, called a "mainframe," was centrally located within an organization. The central location simplified maintenance and the security of the mainframe computer, only the rooms containing a mainframe computer needed to be secured (Witkin, 1995). Security was even less of an issue because access to the mainframe was only allowed by a small group of computer operators. An attack would have to be initiated by one of the few employees who had access to the system.

In the late 1970s the computing process was decentralized by smaller and cheaper information systems, called PCs (Witkin, 1995). More people now had access to information processing, but it was at the cost of reduced security. More information systems meant increased vulnerability. Security was no longer centralized to a single physical location and accountability became increasingly difficult with the growing number of PC users. Internal threats, such as disgruntled employees, were the largest threat to an information system.

Initially, the only way to share data between PCs was physical media, such as a floppy disk. As PCs became more dispersed throughout an organization users wanted an efficient way to share data (Witkin, 1995). Physical media was a threat to system security, but a bigger threat occurred when user demand led to the interconnection of multiple information systems to form networks. This allowed transfer of information directly between information systems. The addition of each new connection added another potential vulnerability or threat to the overall system. Manual auditing became increasingly difficult because of the amount of information on a system plus the amount

of information being passed between systems.

Network security was again degraded when the geographical limitations of potential attackers were removed through distributed architectures which allowed more users access to information systems from vast distances. The initial distributed architecture was called a local area network (LAN) which encompassed an area no larger than the size of a city block. The use of LANs eventually led to the development of a network that permitted communication within an area the size of an entire city. These types of networks were called Metropolitan Area Networks (MAN) (Witkin, 1995). Eventually global communication networks were developed, called Wide Area Networks (WAN). Communication protocols for the WANs, MANs, and LANs were not standardized, separate phone lines were leased to handle the data transfer for each network. Therefore an attacker would have to know what type of communication was being used on a network and also be able to gain physical access to the network communication lines.

Internet Technology

The goal of the Advanced Research Projects Agency Network (ARPANET) in 1969 was to develop a common communications protocol to increase the speed and robustness of government digital communication networks. The security for ARPANET wasn't a primary concern because only U.S. government agencies had access to it. In 1986 the ARPANET was handed over to the National Science Foundation (NSF) and expanded to include users from the private sector forming what was called the "Internet."

The Internet expanded quickly as organizations realized its benefits. Many

advantages exist for using the Internet over a WAN, such as cost and convenience, the primary disadvantage being security. A connection to the existing internet is considerably cheaper than leasing the communication lines necessary for a WAN, but this meant openly sharing communication lines. The Internet is also more durable then a WAN because of the multitude of interconnections message traffic can be routed through, yet the interconnections threaten security since all other users are connected to the same communication lines (Lipson, 2002).

In late 1988 the first reported major incident occurred on the Internet. The incident was a computer program called a worm which caused information systems to lockup fooling them into attempting to connect to nonexistent IP addresses. This effectively shut down use of the Internet. Even with the devastating effects caused by the single malicious attack the advantages of using the Internet outweigh the risk. This is true even as the number of users grew and the potential for malicious activity became more of a concern. To make matters worse, security was difficult to improve upon because Internet standards had already been well established (Lipson, 2002).

Intrusion Detection

Intrusion detection became necessary in the early 1970s when network connectivity began to threaten information security (McHugh, 2001). Intrusion detection was initially done through manual auditing of computer logs. Manual auditing worked well during the 1970s because computer systems could be accessed only by a small group of users and computer logs were small enough to be manually inspected. However, as the amount of data increased and the number of connections grew the task of manual

auditing became effectively inconceivable (McHugh, 2001).

As the threat of network attacks grew, organizations began to implement additional security measures in addition to manual auditing to counteract the threat. A prevalent tool used to counteract the threat of attacks was the intrusion detection system (IDS). IDSs are automated auditing tools used to collect and sort data such as logs or transmissions from a network or computer system then alert administrators when that data contain characteristics of an intrusion (McHugh, 2001). The fundamental method of comparing known attack data with current network traffic data for intrusion detection, around since the early 1980s, is still the primary basis for intrusion detection today. Unfortunately, IDSs are too slow to keep up with network traffic and unreliable when distinguishing new types of attacks (Allen et. al, 2000). Because of there limitations, attacks detected by an IDS on an information system can only be considered a portion of the actual number of attacks.

Past Incident Prediction Research

The problem of determining a correlation among foreign media coverage of military events and network incidents is specific yet includes a wide range of topics. Though most information relating to this research problem did not pertain to correlation analysis the few existing research articles found using incident data to predict future incidents were the basis of this research.

There are three research documents that address incident analysis as a method to reduce future incidents: Ginn, 2001; Yurcik, Loomis, and Korzyk, 2000; and Korzyk, 1998. This is understandable considering how narrow the topic is and the lack of valid

and reliable metrics in the past. Each paper focused on the reactive nature of network security and the desire to create more proactive security tools and procedures. Although this research considers a much wider range of potential effects of the foreign media and incident data then attempted before, the existing research provided a solid basis for this study.

Korzyk (1998) developed a forecast model using historical incident data to predict future incident volume. A forecasting model has many similarities to a correlation analysis, both require use of statistical analysis to compare past data and find trends or similarities. Once significant trends are discovered the data can be used to create a model and predict future trends or determine the causes of the trends. Korzyk's (1998) research found a slight seasonality correlation and additional trends in the incident data. He used several forecasting models to find the best fit for predicting incident data, but none were successful enough to be of significant use. Korzyk's notice of incident trends did show evidence some types of correlations and predictions may exist for incident data.

Yurcik, Loomis, and Korzyk (2000) focused their research on how incidents were detected and reported. Several problems exist with analyzing incident data: growth of the Internet, changing technology, low reporting rates for security incidents, false alarms rates, and the changing nature of Internet attacks (Yurcik, et. al, 2000). The problems can be minimized if proper metrics are used. The following is a list of metrics suggested by Yurcik et. al (2000):

- Type of Internet attack based on a common taxonomy
- Number/percentage of Internet attack frequency growth
- Number/percentage of detected/undetected Internet attacks
- Number/percentage of successful/unsuccessful Internet attacks

- Number/percentage of reported/unreported Internet attacks
- Number/percentage of automated Internet attacks
- Types of automated Internet attacks – tools used/ports probed
- Stationarity of Internet attacks over time (day/day of week/month/year/season)
- Duration of Internet attacks (day/month/year)
- Number of hosts involved in Internet attacks
- Damage Cost estimate for distinct Internet attacks
- Geographical location (physical and virtual mapping) of Internet attacks
- Targeted systems (location/organization/vendor/operating system)

This is a list of potential metrics that would help prevent incidents, not an actual list of current metrics. Most organizations have different lists of metrics which depends on their methods of incident reporting (Yurcik et. al, 2000). The lack of a standard set of network incident metrics hinders the ability to determine if correlations exist among the combined incident data. Furthermore, advanced intrusion tools and distributive attack techniques allow attacks to be performed in a chaotic manner in which a correlation would be harder to discern (Yurcik et. al, 2000).

Patrick Ginn (2001) did a regression analysis and discovered no correlation between incidents tracked by the Fleet Information Warfare Center and United States foreign media exposure for the year 1999. He used the IN-SPIRE software to quantify the number of media reports per week related to the United States. However, a regression test does not work well when determining a correlation with highly fluctuating data sets. Also, Ginn (2001) only used foreign media documents that contained the exact phrase "United States" and combined the incident data from categories I, II, III, IV, VI, and VI for his analysis. Incident analysis methods and intrusion detection techniques during this time were not well established. As a result incident data were not as well documented. Fortunately for this research, the methods used by the DoD to analyze and

categorize intrusions have become much more consistent in recent years.

DoD Network Incident Metrics

Network incident data used in this research was attained from the Joint CERT Database (JCD). The JCD is a collection of various defense agency incident data used by NetDefense. NetDefense is also known as the Department of Defense Computer Emergency Response Team (DoD CERT) who falls under the Joint Task Force Global Network Operations (JTF-GNO) agency which works to protect, defend, and restore elements of the global information grid. The JCD incident data contains eight categories: unauthorized access, unauthorized user access, unsuccessful attempted access, denial of service, poor security practices, unauthorized probe, malicious logic, and unknown (Table 1).

Table 1: Incident Category Description

Category	Description
I	Unauthorized Root Access
II	Unauthorized User Access
III	Attempted Access
IV	Denial of Service
V	Poor Security Practice
VI	Probe or Scan
VII	Malicious Code
VIII	Unknown

Each category is specific to a type of network incident described as follows. Unauthorized root access and unauthorized user access describe the type of privileges an attacker gains for an information system. They encompass a range of incidents from improperly logging into a user's account, such as a hacker logging into a legitimate user's

account, to obtaining unauthorized access to files and directories. Unauthorized root access incidents occur when access is gained to a system with root privileges without authorization. Unauthorized user access incidents occur when access with user privileges is gained to a system without authorization.

Unsuccessful attempted access is the next type of network incident tracked by the DoD. Unsuccessful attempted access is defined as repeated attempts to gain access as root or user on the same information system from the same source. Tracking these types of incidents shows how successful safeguards of DoD systems are in incident prevention and produce information on attacks volume.

Successful disruptions of network operations are labeled “denial of service” incidents. More specifically, denial of service incidents are unauthorized actions which preempt or prevent any part of an information system from functioning properly, such actions include destruction, modification, or degrade performance of a system or network affecting the mission, business, or function of an organization.

An unauthorized probe is any attempt to gather information about an automated information system or its users on-line by scanning a site and accessing ports through operating system vulnerabilities. Probes can be used by attackers to find out information about a network for a future or ongoing attack.

Finally, the category of malicious logic incidents are the most obvious and disruptive attacks caused by hidden hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose. Malicious logic software is self-replicating and disseminated by being attached to or mimicking authorized

computer system files, such as a Trojan horse, worm, malicious scripting, or a logic bomb. The effects of malicious logic attacks include but are not limited to simple monitoring of traffic, corruption of information, disclosure of information, theft of service, and automated backdoors with full system rights.

The two categories "poor security practice" and "unknown" can be separated from the other six categories for the following reasons. "Poor security practice" metrics are actions of the victim not the attacker, such as uninstalled software security patches. "Unknown" incidents are yet to be classified into one of the other seven categories, therefore "unknown" is not an actual incident category itself. However, most "unknown" incidents are later reclassified into "denial of service" incidents (Svetlev, 2004). Therefore, because neither poor security practice nor unknown incidents can be, at least yet, considered direct actions of an attacker the data from these categories are not included in this research.

Howard's (1997) original taxonomy of network attacks divides the method of access to a network into two groups of users, those that are not authorized access and those that are not authorized use. However, Howard and Longstaff's 1998 taxonomy (Figure 4) does not directly distinguish between these two categories. Rather, Howard and Longstaff (1998) eliminate the access category and refer to attacks as having unauthorized results. This improves the mutually exclusive and collectively exhaustive properties of their taxonomy but fails to address the importance of access metrics, as was verified by Daigle (2001). Knowledge is gained from breaking down access characteristics of network attacks.

Howard and Longstaff's (1998) taxonomy continues to segregate network attacks by their unauthorized results: increased access, disclosure of information, corruption of information, denial of service, and theft of information. One of these results (denial of service) is tracked by the "denial of service" DoD incident metric. Unauthorized root access, unauthorized user access, and attempted access DoD incident metrics track the level of increased access addressed in the taxonomy. Unfortunately, DoD incident metrics do not break down further which category of incidents address the disclosure, corruption, or theft of information. While this does limit the scope of this research, it is not necessary to determine if a relationship exists between foreign news media reports of DoD events and network attacks against DoD systems.

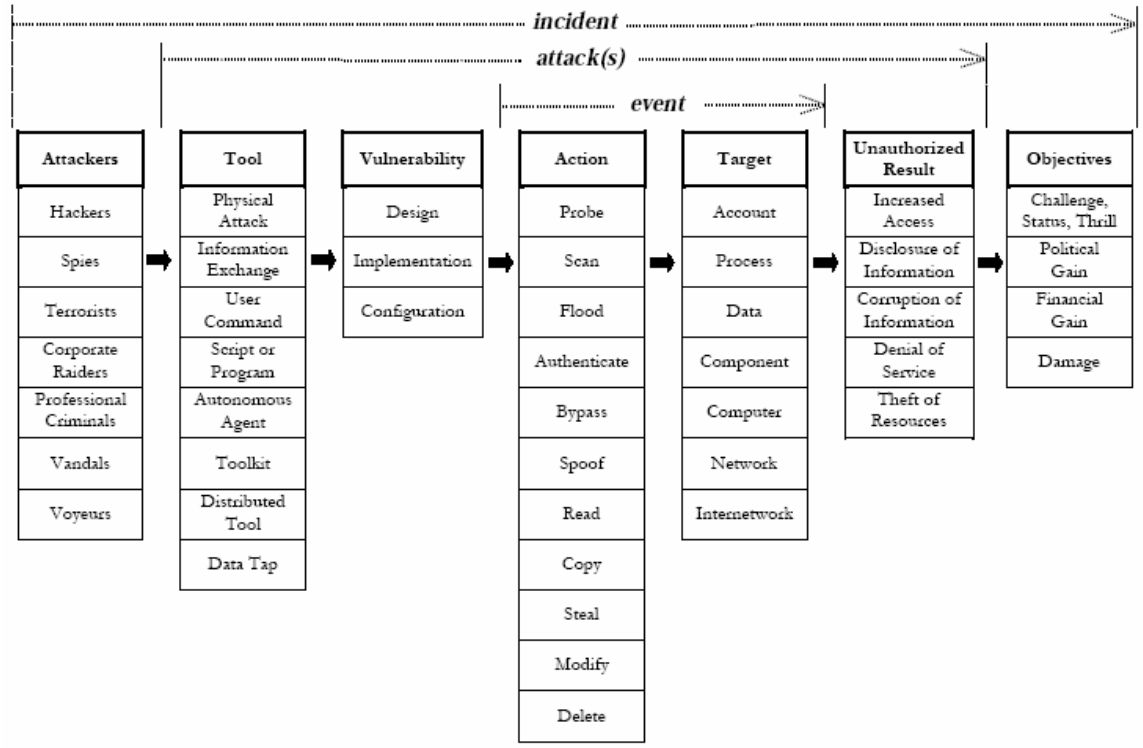

Figure 4: 1998 Computer and Network Incident Taxonomy

The Motivations of a Network Attacker

As can be seen in Howard and Longstaff's (1998) taxonomy the objectives for network attacks include "challenge, status, thrill," "political gain," "financial gain," and "damage." "Challenge, status, and thrill" is a very broad category which encompasses attacks that may mean no harm, but are done simply to break through the security of a network system. By contrast, the other motivations are meant to cause either direct or indirect damage to the system under attack. The purpose of political gain is to gather information and at the same time deny that information from opponents for the purpose of gaining an advantage for one's own government. Motivation for financial gain differs from political gain because the objective pertains to wealth. Financial gain attacks can consist of monetary compensation for the safe return of stolen information similar to a ransom, or steeling information for increased competitive advantage or market share. Motivation to cause damage results in the types of events seen readily in the media. "Damage" motivated attacks, such as denial of service or malicious logic attacks are not as focused on specific networks. Rather, these attacks start at any system on a network and can spread to all other systems connected to that network. "Damage" motivated attacks are clarified in depth by Kleen (2001) in her thesis, "A Case Study on Malicious Hackers."

A trend in the categorization of motivations which is taken to an extreme by Jordan and Taylor (1998) is a focus on challenge and status as the primary reasons for network attacks. The type of hackers that perform network attacks for challenge and status consist of individuals with an internet connection and the few tools necessary to

connect into an unauthorized network. This class of attacker is composed of members of the general public who take the time to learn about the tools and techniques use to perform network attacks.

Network attack motivations are universal to employees and non-employees. However, non-employees have additional physical or electronic security measures to bypass before they can gain access to a system. Employees already have some access to their organization's network, which is one reason why the majority of successful attacks are perpetrated by employees.

DoD Network Policy

There are three forms of policy governing networks within the DoD; they cover access rights to DoD systems by both DoD personnel and authorized non-DoD personnel, security of DoD systems, and network connections to and between DoD systems.

DoD Policy on Access to Information

Because the DoD's function is the security of the nation and its people the information held within the DoD is the property of U.S. citizens. Therefore, this section covers government policy on access to DoD information in two parts, one for the general public, the other for DoD employees.

Public Access to Information

DoDD 5400.7 Freedom of Information Act (FOIA) states that in order to promote public trust, the maximum amount of information about DoD activities should be easily accessible by any U.S. citizen who requests it. The FOIA allows complete disclosure of DoD information and activities to the general public, with the exception of any

information that is private to individuals within the DoD, subject to classification, or deemed sensitive for reasons of national security. DoD Directive (DoDD) 5230.9, which clarifies the procedures for declassifying information for public release, states that clear and accurate information be declassified and distributed as soon as is possible to aid the public's understanding of DoD actions and policy.

DoD policy affirms the public should be allowed access to all DoD information not subject to restrictions for national security. However, DoDD 5230.9 and the FOIA state access to DoD information must be under the control of DoD personnel. Unauthorized access by members of the public to DoD unclassified public information is considered an attack. To avoid any potential problems a request for DoD information must be handled through the proper procedures.

DoD Personnel Access to Information

DoDD 5200.1 and DoDD 8500.1 require DoD personnel be educated and trained in the protection and classification of computerized classified information and network defense techniques. Education and training also clarify the responsibilities of the individual member in how to prevent unauthorized disclosure of information.

The proper control of information by DoD members is well established in DoD policy. Guidance on who should be allowed access to sensitive information is outlined in DoDD 5200.2, DoDD 5200.2R, and DoDD 8500.1. These directives state that no person should be allowed assess to classified information unless it is in the interest of the nation's security. Finally, DoDD 5200.2R stipulates the requirement for all DoD personnel to have appropriate background checks and training before being granted

access to DoD computer or network systems.

Information System Security Policy

DoD Instruction (DoDI) 5200.40 applies directly to the security of DoD information systems. DoDI 5200.40 establishes a process to certify and accredit information systems and verify each one has been checked for security flaws as well as has an acceptable level of risk. The certification and accreditation (C&A) process measures security by assessing the level of risk of each DoD owned computer system and the significance of that system to DoD operations. Tools to measure the significance of each system and determine appropriate security measures are contained in DoDI 5200.40 as well. The C&A process includes annual evaluations for each system to ensure all irrelevant information is removed or new information is included on the most recent C&A.

The C&A process places responsibility on the designated approving authority (DAA). The DAA is an individual who must have the authority to accept responsibility and risk of the system. Usually the DAA is an O-6 grade officer or higher assigned command of an organization which is responsible for the information system. The DAA verifies and signs that a satisfactory C&A was accomplished. When this process is carried out properly the information system is considered secured.

Network Connection Policy

DoD networks are allowed connection to outside organizations, such as international allies, other government agencies, and civilian organizations deemed necessary for mission accomplishment. Outside access should only be completed with

the approval of the network DAA who has the responsibility to verify the connection requirements are necessary for mission accomplishment and are within an acceptable level of risk (DoD Instruction 8500.1). The term “acceptable level of risk” is rather obscure for a system connected to an inherently varying level of risk. DoDI 5200.40 and 8510.1M quantify external connection risk by evaluating several factors of both the risk in using a particular system and the criticality of that system in support of DoD operations. The more critical a system is to the DoD, such as saving lives and money, the less risk the DoD will take with that system. Of course, risk can be reduced by increasing security measures, such as minimizing network connections.

News Media and DoD Relationship

The First Amendment of the U.S. Constitution states, “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” How much freedom the press is allowed is difficult to interpret. Through time our nation's press, DoD policy regarding the press, and DoD operations have adapted to one another in hope of reaching a happy medium.

History of the News Media and the U.S. Military

Both DoD and media personnel accept their relationship as vital to maintain our nation’s freedom (Aukofer and Lawrence 1995). Maj Raymond Hill, Jr. (1997) referred to the media as the vital link between Carl von Clausewitz Remarkable Trinity of the people, their government, and their military. This section overviews the history between

the military and its link to the people, the media.

The Formation of Today's Relationship

For the U.S. the earliest form of mass media was a majority of opinionated articles on a single sheet of paper during the Revolutionary War (McHugh, 1997). These articles didn't have content restrictions, or rules governing content validity. The uses of the press were soon found to be beneficial in spreading information, but also a hindrance when the information was biased or misleading.

The press was more prominent in the Civil War where reporters were included on the battlefield for the first time in U.S. history. The motivation for the media was the public's growing desire for information on the war. So strong was this desire that the military didn't dare interfere with the media for fear a public uproar. At this point in time the speed news traveled became faster then military movements, meaning opposing forces could gain significant intelligence from public news reports (Hill, 1997). The military had relied on a trusting relationship to keep information like troop movements and battle plans safe from publication. Eventually this trust broke down and the press published vital operational information setting up the need for U.S. Government control of news media actions.

The media's access to information remained under government control through the first and second world wars. Regardless of the restrictions, at the time the public and the media were extremely patriotic so few protests were ever made. The harmony ended years later during the Vietnam War when censorship was lifted and the media's coverage began including subject matter that supporters of the military believed was biased and

meant to persuade the public to force a premature end to the war. The result was a bitter relationship between the media and military, both accusing the other of providing inaccurate or biased information (McHugh, 1997).

To improve the relationship the military began to set policy where news media involvement became a part of operational planning (Aukofer and Lawrence, 1995). However, most operational planners chose to exclude the media because of their hard feelings caused by Vietnam War coverage. Most plans continued excluding the needs of the media through the 70's and early 80's. During the Gulf War of the early 1990's, military plans began to include the requirements for media coverage, but still failed to completely encompass the needs of the media. The media also failed to fully understand the military. Many military members complained of media reporters' lack of knowledge concerning the military's operations and structure (Aukofer and Lawrence, 1995). The military continues to improving its relationship with the media today by establishing rules and principles for both the military and the media to follow, relying on trust to maintain its effectiveness.

Significance of the Media in the United States

The early press during the Revolutionary War was rudimentary in its collection of information as well as the reporting of that information. Newspapers were only a page long and took hours to print a significant number of copies (McHugh, 1997). Although news was limited, it was thoroughly read by the public (Snyder, 2003). The news media had difficulty getting information because the slow communication links between where news was made and where it was published. In the next two centuries a revolution took

place that drastically reduced the amount of time it took news reports to reach the public.

The public's desire for news created commercial competition which pushed advancements in communication and coverage. The media started to use a reporting technique where a network of affiliates across the nation would be used to cover a large geographical area at one time. The telegraph and dedicated pony express sped news across the nation allowing the public to get news of a battle while the battle ensued during the Civil War. Competition between publishers pushed reporters to put accuracy and security below the need to get an article published first (Snyder, 2003) (McHugh, 1997). No controls were in place to prevent reporter bias or inaccuracy until the first and second world wars when heavy censorship was placed on the media. The patriotic news media accepted the censorship as a necessity of war (Snyder, 2003).

The speed of reporting was greatly increased with the invention of the radio, which became the primary source of news during WWII providing live war coverage from across the globe. News coverage traveled ever greater distances through a robust radio communications system providing faster coverage of ongoing events. However, the visualization of the news coverage was still primarily limited to the imagination of the public and the restrictions placed on the reporters.

Television coverage of war began with Vietnam and eliminated the need for the public to imagine what war looked like. In addition, most restrictions were lifted and reporters were free to cover events as they saw fit. Live news coverage was still restricted to radio, but video taken from earlier in the day made that night's evening news broadcast. The American public was not ready for the realities of war and was shocked

by what they saw (Snyder, 2003). Eventually the graphic depictions of war and inconsistencies between media reports and government statements resulted in a decline in public support for the Vietnam War (Snyder, 2003). Events like Vietnam demonstrated the use of the media as a tool in asynchronous warfare. Public opinion was affected by news media coverage which resulted in a U.S. withdraw, in effect allowing the adversary to win a battle.

The amount of information readily accessible by the public continued to increase as television coverage became live with satellite technology and internet coverage during the early 1990's in the Gulf War. Technology and reporting techniques successfully brought the war into the American home.

As a result of decreased time for information to reach the public, the amount of time the DoD has to make decisions is reduced. Public outcry is a major influence on DoD operations and media reports can affect the public's opinion on DoD operations. When media reports do not include all the facts or distort the truth the DoD may not have the time to successfully educate the public on the nature of an operation, which may result in an operation being prematurely cancelled (O'Boyle, 2000). Once the public has a set view of a situation it becomes increasingly difficult to change that view. Many myths have resulted in the misuse of the media to include the effect the Vietnam War has had on Vietnam veterans. In this example several reports state Vietnam veterans are more likely to commit suicide then the rest of the population, which is incorrect and based on false statistics (O'Boyle, 2000). Even though the statistics are not substantiated the myth remains, so the DoD must remain cognizant of news media effects.

How the Military Adapted to News Media

During the time when colonial America was fighting for its independence, military leaders began to see the use of the media as a tool to influence public opinion, including the opinions of military personnel (Snyder, 2003). The colonial military took control of any press who didn't support their cause thus enforcing a positive influence on public and troop support.

The luxury of news media control was diminished by a more substantial media during the Civil War. As a result the military attempted to contain the flow of information by controlling telegraph lines, restricting the media's access to military information, and physically shutting down any publisher who chose to distribute sensitive or classified information (Snyder, 2003). During the Civil War military leaders realized their lack of guidance on how to deal the media. After the Civil War military policy was written on how military members should deal with the media. In addition, training was provided to standardize interactions military members had with the news media. Further efforts in dealing with the media and community resulted in the creation of a public affairs office whose responsibility was relaying information between military leaders and the media, or public.

WWI became a war that was covered under massive censorship. The Espionage Act in 1917 and Enemy Sedition Act of 1918 made reporting disloyal information illegal. President Woodrow Wilson issued executive orders which gave the military control of the media. The military used this control to add a requirement for war reporters to gain accreditation before being allowed access to the field. The accreditation ensured the

reporter practiced nonbiased reporting and kept sensitive information from being published. The government also used the media to increase public support for the war producing a massive propaganda campaign against Germany (Snyder, 2003). Together, media censorship and anti German propaganda ensured public support throughout WWI.

During WWII, self imposed censorship was employed. The self-imposed censorship worked well due to the high level of patriotism (Aukofer and Lawrence, 1995). Due to some of the restrictions on reporters, during WWII the concepts for media pools and imbedded reporting were created. Media pools came about because of the limited availability of radio transmission facilities and abundance of media reporters (Aukofer and Lawrence, 1995). One reporter's transmission would be broadcast by several networks. Imbedded reporting came about with combat correspondents. Combat correspondents were journalists who volunteered to enlist in the Marines and report as a member of a military unit. Even with the new developments in war reporting, every report was run through a censorship board before publication throughout the Second World War.

The military initially gave in to the demands of the public and decided to eliminate all forms of censorship during the Korean War, but eventually went back to heavy censorship. Censorship for the Korean War included information that hindered the security of military operations and military members, deteriorated moral, or embarrassed the military or its allies (Aukofer and Lawrence, 1995). The latter two restrictions were eventually eliminated in later wars because they were found to prevent free speech.

The Vietnam War, on the other hand, did not impose censorship throughout the

war. The media's coverage of the Vietnam War resulted in a severe reduction in public support and consequentially resulted in the United States backing out of the war. Not so much because of how the news media reported the war, but how the public realized the cost of the war (Aukofer and Lawrence 1995). Public support was continually degraded as government reports of progress in the war failed to coincide with news reports of enemy actions. After the Vietnam War several DoD directives were developed concerning the need to enhance public affairs. The media was to be given maximum support in their efforts by the military, and the major combatant commands were responsible for maintenance of this support.

However, the aid to the media was primarily considered a function of Public Affairs personnel. Because of their reliance on the Public Affairs office commanders hardly ever considered the needs of the media when devising military operations and assumed any media needs could be handled independently by Public Affairs personnel (Aukofer and Lawrence, 1995). This resulted in the complete exclusion of all media for the first two days of the Grenada conflict. Afterwards, a DoD National Media Pool (DNMP) first conceived during the WWII was initiated to help ease logistical concerns for including media in war planning. Military commanders misunderstood the intent of the DNMP and thought it would eliminate any need to include the media in military operations. The result was another initial exclusion of the news media from the conflict in Panama.

Currently, DoD policy is better understood so military planners can do a better job including the needs of the news media in military operations. However, new problems

have surfaced. Conflicts are harder to cover with round the clock operations and precision warfare. Media reporters can only be assured coverage if they deploy with the military units conducting the attacks. Reporters independently covering a conflict may become a liability to the military or are unlikely to witness any ongoing operations (Aukofer and Lawrence, 1995).

DoD Information Disclosure Policy

One aspect of this research is whether or not too much information is being released to the public causing an increase in network incidents. It is not the focus of this research to determine causation, but it is helpful to review the DoD directives and instructions pertaining to the release information within and outside the DoD. There are three aspects of these documents of concern: U.S. information disclosure, foreign information disclosure, and the process of information classification.

U.S. Information Disclosure

The discloser of DoD information to the U.S. public involves three key factors: responsibility for the information, methods of disclosing the information, and DoD news media support to ensure effective coverage of the information. Responsibility for information disclosure lies with the Assistant to the Secretary of Defense for Public Affairs (ATSD(PA)), commanders, and Public Affairs personnel.

The ATSD(PA) advises the Secretary and the Deputy Secretary of Defense on matters concerning news media relations, public information, community relations, and public affairs. ATSD(PA) is the final approval for all policies, plans, programs, and actions that have operational implications. ATSD(PA) acts as the sole spokesperson and

release authority for DoD information and audiovisual materials to news media representatives. This includes establishing procedures for the administrative management, activation, and direction of the DoD National Media Pool. Furthermore, the ATSD(PA) supports DoD objectives and operations by developing policies, plans, and programs to ensure free flow of news and information to the news media and general public while maintaining national security constraints laid out in Executive Order 12958, "Classified National Security Information," 1995.

DoDI 5400.14 requires the commander of the combatant command to include public affairs needs in all DoD operations. The needs of the media must be considered from the earliest stages of an operation. DoDI 5400.14 clarifies the needs of the news media which include personnel, transportation, facilities, equipment, and communication assets. With the help of Public Affairs a Joint Information Bureau (JIB) fulfills some of these needs by acting as the interface between the media and U.S. military forces during joint operations. JIBs aid the commander in establishing a healthy relationship with the media and ensuring the media's needs are being met. Public Affairs tasks include preparing reports for anticipated media questioning, setting policy, and preparing news statements. Highest priority in media relations is placed on the training and transportation of public affairs support. This is to ensure effective communication between public affairs personnel and the news media. Support to the media should be a continuous 24 hours a day task. The ultimate goal of Public Affairs actions are to provide the media with as complete a picture of the operation as is possible without hindering operations.

The DoD is required to support and cooperate in programs involving relations with the public, national associations, and non-governmental organizations consistent with DoD Directive 5410.18 and DoD Instruction 5410.19. Methods to disclose information include media pools, standard media reporting, written statements, public announcements, and the like. The most direct method of gaining information is directly from the source where the media is also allowed full access to DoD units and personnel involved in an operation. The personal safety of correspondents must be considered when being allowed on the battleground, but it is not a reason for excluding the news media from military operations. Access to personnel does take exception to those DoD personnel who need to remain anonymous for operational safety. In addition to news reports and interviews the DoD also provides documentary products for release to the news media produced by Joint Combat Camera.

Ground rules must be fully developed by the combatant commander and understood for the civilian news media to abide by. The DoD established a set of guidelines to help DoD personnel better understand what the needs of the media are and how to establish a successful relationship. Figure 5 depicts the DoD media guidelines for open and independent DoD operation reporting.

Figure 5: Department of Defense Media Guidelines (JP 3-61, 1997)

Foreign Information Disclosure

Joint Publication (JP) 3-13 (1998) reinforces guidelines for U.S. media relations as with standard DoD media policy. However, for certain operations foreign media can be an effective way to affect opposition members to include its leadership. This is true because DoD policy regarding the disclosure of information to foreign nations is separate from local policy, such as the ability to conduct information operations. The three forms of DoD information operations which affect foreign media are physiological operations (PSYOP), civil military operations (CMO), and military deception operations. All three forms of operations must work with each other to eliminate or minimize contradictions

and maintain credibility with the agencies and populations of foreign nations and the U.S. (JP 3.61, 1997).

CMO and PSYOP manipulate information to influence foreign agencies and populations (JP 3-57, 2001; JP 3-53, 2003). CMO is meant only to positively influence foreign populations, whereas PSYOP can have both positive and negative affects and is meant to directly influence foreign governments, leadership, military members. etc. Military deception as a tool used to create an advantage over a military adversary by deliberately misleading their leadership with false information about U.S. forces (JP 3-58, 1996). Deception operations, PA, CMO, and PSYOPS should be coordinated through one another prior to there use to ensure contradictory information isn't released which could discredit the operation. It is against DoD policy to misinform the U.S. public by any means therefore military deception, PSYOPS, and CMO is strictly to be used against non U.S. entities (JP 3-13, 1998).

DoD Information Classification Policy

The release of official DoD information to the public is limited only as necessary to safeguard information in the interest of national security or other legitimate governmental interest, as authorized by official government directives. It is DoD policy that accurate and timely information is made available to the public, the Congress, and the news media to help the analysis and understanding of defense strategy and national security issues. Any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance by appropriate security review

and Public Affairs offices prior to release (DODD 5230.9, 1996).

The primary method to prevent classified and sensitive information from being reported is through the practice of "security at the source" where each individual is responsible to ensure no classified information is disclosed. Other safeguards such as media ground rules and formal security reviews are not to be relied upon for safeguarding information (DoDI 5400.14, 1996).

Prior its release any information must be classified either top secret, secret, confidential, or unclassified. To be considered for classification above unclassified the information is required to include one or more of the following (Executive Order 12958, 1995):

1. Military plans, weapons systems, or operations.
2. Foreign government information.
3. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
4. Foreign relations or foreign activities of the United States, including confidential sources.
5. Scientific, technological, or economic matters relating to the national security.
6. United States Government programs for safeguarding nuclear materials or facilities.
7. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

On the other hand, in no case shall information be classified for the following reasons (Executive Order 12958, 1995):

1. To conceal violations of law, inefficiency, or administrative error.
2. To prevent embarrassment to a person, organization, or agency.
3. To restrain competition.
4. To prevent or delay the release of information that does not require protection in the interest of national security.

Other rules prevent certain information from being classified as well, such as basic scientific research not clearly related to national security may not be classified.

Information may not be reclassified after it has been declassified and released to the public under proper authority. However, if the information has not previously been disclosed to the public, under proper authority information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act.

Another aspect of information security is the disclosure of classified information through a collection of unclassified information. Several separate reports of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the two following criteria:

1. The compilation of information meets the standards for classification under Executive Order 12958, 1995.
2. The classified aspects of the compilation of information are not otherwise revealed in the individual items of information.

DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD forums or media. Clearance shall be granted if classified information is not disclosed, the DoD interests in non-classified areas are not jeopardized, and the author accurately portrays official policy, even if the author takes issue with that policy. Such activity is authorized if:

1. No laws or regulations are violated.
2. Ethical standards and compliance with proper conduct are maintained (covered in DoDD 5500.7 and DoD 5500.7-R).

3. The preparation activities are not done during normal duty hours or with the use of DoD facilities, property, or personnel except as authorized by DoDD 5500.7 and DoD 5500.7-R.
4. The author does not use official DoD information generally not available to the public and which would not be released under DoD 5400.7-R.

It is the responsibility of the Director, Washington Headquarters Services in conjunction with the heads of the DoD components to ensure compliance with the above directives. All are needed to provide assistance and recommendations on what policy and security implications may exist for information proposed for public disclosure. Whether or not these constraints are enough to prevent sensitive information from causing network attacks is a part of what this thesis is intended to discover.

Summary

The purpose of chapter II was to review current literature pertaining to network attacks against DoD networks and review aspects of how network incidents could be correlated to foreign news media coverage of DoD events. Computer technology combined with networking technology has spread the ability to attack computer systems from a few knowledgeable individuals with direct access to the system to just about anyone with an internet connection. Currently the advantages of using the internet outweigh the risks of network attacks. The risk of network attack can be reduced through the use of information assurance tools such as IDS. However, attack detection is difficult because networking technology wasn't designed well for security and IDSs are limited in resources and capabilities.

The problem of handling attacks is made worse by the difficulty in classifying network attacks. Not being able to distinguish separate attacks consistently leads to

misrepresentation of data obscuring possible valuable information. A better understanding of what causes individual to perform network attacks could help create more effective tools or revise DoD policy to reduce the number of attacks. Several motivations exist for attacks conducted against DoD networks. DoD policy should both limit the agitation of any negative motivations and increase the ability of the DoD to react effectively against an attack.

DoD operations already consider the needs and the effect news media reports have on those DoD operations. The extent of the affect media reports have on DoD operations is unclear and under constant ridicule. The public has a right to know the actions being conducted by their military, but the security of DoD assets needs to be weighed carefully against the rights of the public. Similar circumstances revolve around foreign media, however the U.S. military is not restricted in the use of information operations against foreign nations. Therefore it would be possible to manipulate information disclosed to foreign sources in an effort to improve DoD network defenses.

III. Methodology Outline

Chapter Overview

This chapter details how the relationship between foreign news media reports covering U.S. military events and network incidents against DoD systems is examined. The first section describes the population of interest, the portion of the population collected for this research, where the data are acquired, and how the data are manipulated for the correlation test to be conducted. Next, definitions and validation of the dependent variable (DoD network incidents) and independent variables (foreign news media reports) are given. This chapter concludes with a description of the procedures used to answer the investigative questions presented in Chapter I.

Data Collection

All data in this research are obtained from the Foreign Broadcast Information Service (FBIS) and the DoD NetDefense. Each organization maintains an archive of data for the past several years including the dates of this study, 1 January 2002 through 30 June 2004. Data from NetDefense was collected and transcribed into a Microsoft Excel spreadsheet suitable for statistical analysis. As is described below, data from FBIS had to be analyzed and quantified using the IN-SPIRE software data mining tool before being included in the MS Excel spreadsheet as well. The raw data from both sources are considered For Official Use Only (FOUO) and are therefore not readily available to the public.

Table 2: Statistics on the Daily Number of FBIS Foreign News Media Reports for Each Region

	Central Eurasia	China	East Asia	East Europe	Near East and South Asia	Sub-Saharan Africa	The Americas	West Europe
Total	175618	140931	189773	166732	339623	110172	56941	141583
Average	193	155	208	183	372	121	62	155
Std Dev	105	57	73	77	78	40	23	49

Table 3: Statistics on the Daily Number of DoD Network Incidents for Each Category

	CAT1	CAT2	CAT3	CAT4	CAT6	CAT7
Total	641	584	12552	115	116592	3013
Average	1	1	14	0	128	3
Std Dev	2	2	21	1	47	13

Sample Population

Two groups of data will be analyzed in this research. The first group consists of eight different regions of foreign news media reports (Central Eurasia, China, East Asia, East Europe, Near East and South Asia, Sub-Saharan Africa, The Americas, and West Europe). Media reports for each region are analyzed separately in an attempt to maximize the scope of this research. Domestic news media reports were excluded due to the lack of a comparable data source for domestic reports. The second group will consist of six different categories of network incidents tracked and recorded by NetDefense (unauthorized root access, unauthorized user access, unsuccessful attempted access, denial of service, unauthorized probe, and malicious logic).

FBIS

FBIS offers an in-depth collection of translations and transcriptions of open source information monitored worldwide on such diverse topics as military affairs, politics, the environment, societal issues, economics, and science and technology. The information is obtained by monitoring radio, television, press, periodicals, books and

other sources of unrestricted information such as databases and gray literature. These translations and transcriptions are known collectively as "FBIS Reporting." Information is collected from over 3000 foreign media sources from all over the world. All collected data is translated and converted into basic electronic text format. The data collected is available daily through the FBIS website, or in a bi-monthly update on CD ROM. The latest FBIS bi-monthly updates for the past 30 months, January 2002 through June 2004, will be used as the data source for the foreign news media reports.

NetDefense

The DoD-CERT is presently known as NetDefense, a branch of the Global Network Operations Center, a component of Joint Task Force Global Network Operations (JTF-GNO). The JTF-GNO mission is to protect, defend, and restore the integrity and availability of the essential elements and applications of the Global Information Grid. NetDefense works closely with the following government agencies and non-profit organizations on a daily basis to improve incident tracking, technical assistance, and corrective actions:

1. Army CERT (ACERT
2. Navy CERT (NAVCERT)
3. Navy Information Assurance
4. Air Force CERT (AFCERT)
5. Marine Corps NOSC (MCNOSC)
6. DISA CONUS GNSC
7. DISA PAC-RCERT
8. US CERT
9. DISA EUR-RCERT
10. DISA CENTRAL-RCERT
11. CERT Coordination Center
12. NIPC
13. CIAC
14. FedCIRC

The information collected from the above listed government agencies are used to populate the Joint CERT Database (JCD) which supplies the incident data for this research. Each of the 14 offices communicates with the other offices to improve incident response, however the JCD contains only DoD specific incident data.

When responding to an incident the ideal response for an incident response team includes the following actions:

1. Dispatch the team to the location of the incident.
2. Perform diagnostic tests on the system.
3. Preserve relevant data from the incident.
4. Restore the system to a reliable state.
5. Analyze system security.
6. Return the system to operation and review findings.

This process provides a standard method for each agency to both collect valuable incident data and restore the system. In conjunction with the above process the Armed Services CERTs have established guidelines for categorizing network incidents. The categories range from one to eight and are explained in Table 1 on page 20. As was explained earlier, categories five and eight are excluded from this research because they do not pertain to the correlation being analyzed. Incident response is still a relatively new process, however the efforts spent in the past decade has allowed processes and tools used by incident response teams to detect and categorize incidents to improve greatly. The timeframe of this thesis, January 2002 to June 2004, was chosen because the process of catching and categorizing incidents is best during most recent times and it was the largest sample that could be analyzed in the time allowed for this research.

Data Manipulation

The amount of data used, a total of 1,321,373 foreign news reports and 137,219 DoD network incidents, in this research is too great to be handled in a reasonable amount of time manually. Therefore two software analysis tools are required. One tool, IN-SPIRE, is used to quantify the total number of media reports and media reports containing military events for each day, and subsequently week, of the study from the FBIS archives. Furthermore, IN-SPIRE is able to analyze multiple documents to find common words between those documents which can be used to determine the general content of a set of reports. The other tool is Spearman's Rank Test performed on JMP 5.1 software to determine the statistical significance of any correlations between the data.

Data mining (IN-SPIRE)

SPIRE stands for Spatial Paradigm for Information Recognition and Exploration. The IN letters are used to distinguish the windows version of the software from the UNIX version. IN-SPIRE software can query multiple documents, group documents by content, view the number of documents by a given timeframe, and retrieve a list of the most frequently used keywords in a collection of documents. The two dimensional "Galaxy" visualization display of the IN-SPIRE software, which visually groups a collection of documents by content, is shown in figure 6. By using these functions of IN-SPIRE the relationships of a collection of documents, that may not be immediately obvious through manual observation, can be thoroughly explored.

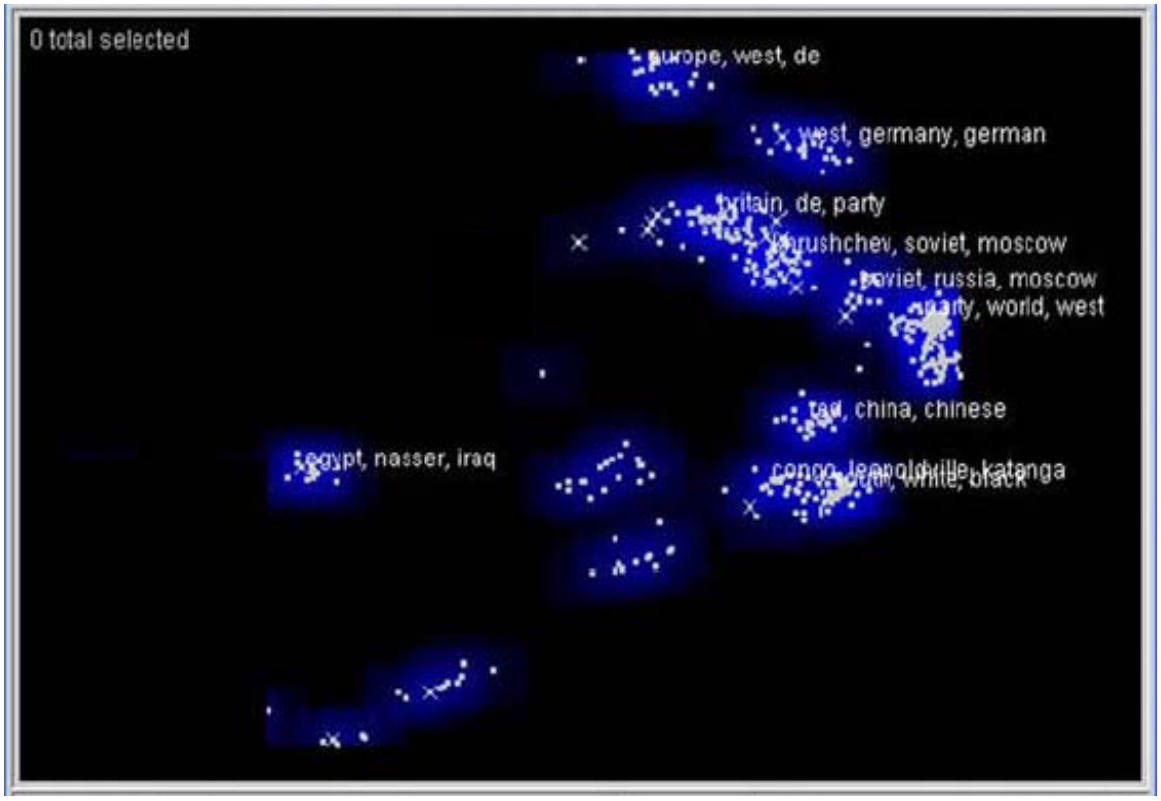

Figure 6: IN-SPIRE Galaxy Visualization Display

The Query tool (Figure 7) provides the ability to search for documents with certain content in a dataset using three different techniques; Vocabulary Work Queries: applying Boolean logic to vocabulary words, Exact Phrase Queries: searching with controlled scope and case sensitivity, and Queries by Example: measuring proximity of words in high-dimensional space. Using this tool is a good way to begin to locate a group of documents that contain specific information in a dataset. By entering a query, a concentration of documents of interest within a larger set of documents can be found quickly. The Query tool also automatically selects and groups documents located by a query so they can be easily separated and studied apart from the rest of the documents. The Grouping tool is a convenient way to organize sets of documents for analysis. By assigning documents to a group, query results can be rapidly retrieved and set operations

can be used to examine the union, difference, and intersection of documents sets.

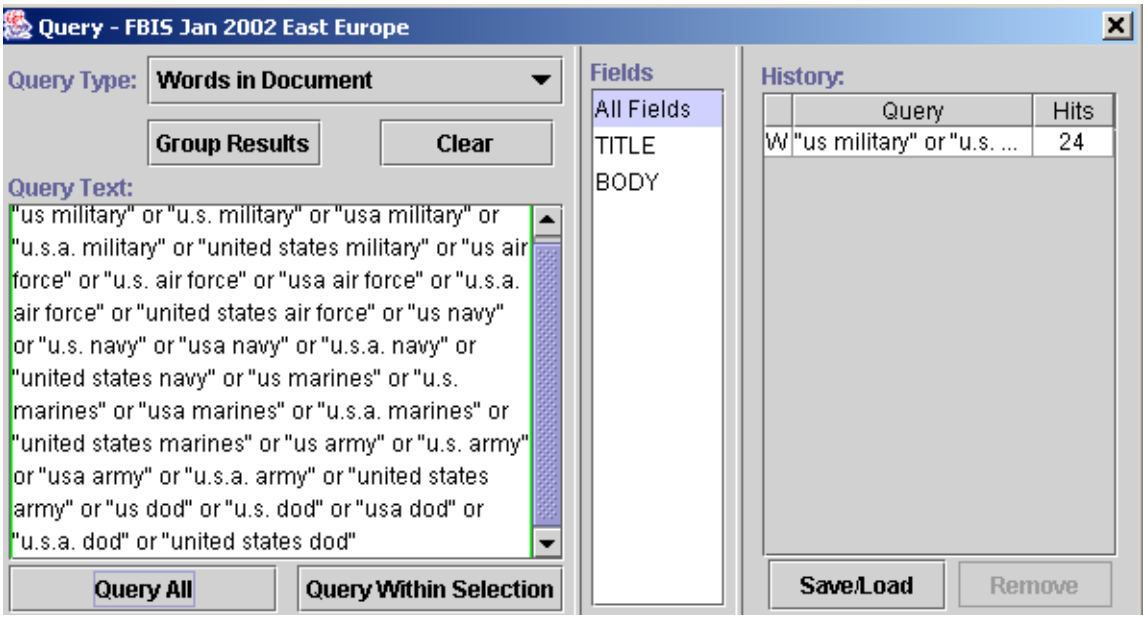

Figure 7: IN-SPIRE Query Tool Display

With the Time Slicer function (Figure 8) a datasets evolution can be explored over time. The Time Slicer works by examining the timestamp in each document and partitioning the dataset into discrete time slice views based on those timestamps. Document counts for each slice of time, from years to minutes, are depicted in a histogram. By interacting with this histogram, an individual can rapidly "slice" through time and watch the information evolve over time, or simply determine the number of documents at a certain point in time. The Time Slicer can partition a dataset only if timestamps are available when the dataset is initially processed, with the granularity of the time slices dependent on the granularity of the timestamp. In this research the required slices of time will be in days.

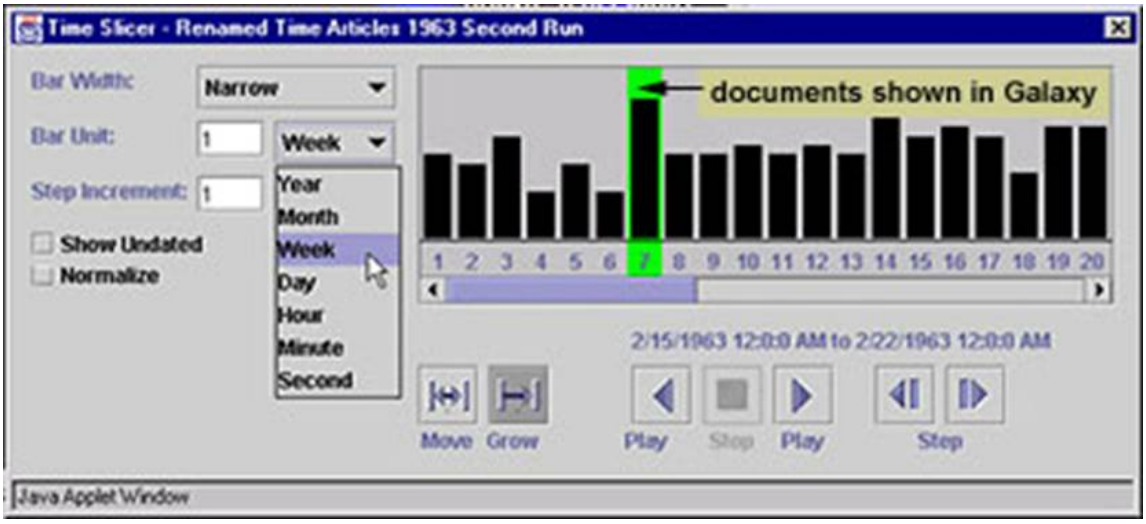

Figure 8: IN-SPIRE Time Slice Tool Display

The IN-SPIRE Gist tool (Figure 9) allows a user to see what words are used most often by a set of documents. The Gist list is a sorting of words in order of the number of documents each word is used in, then alphabetically. The Gist tool can also be used in conjunction with the Query or Stopword tools. The Stopword function is used to remove insignificant words from the analysis of a set of documents. Certain words are already maintained in the Stopword list, such as “the”, “and”, “it”, etc., but additional words determined to be insignificant to a particular analysis can be added with the use of the Stopword tool. With the use of other tools or by itself a Gist is capable of enhancing the exploration and understanding of a set of documents.

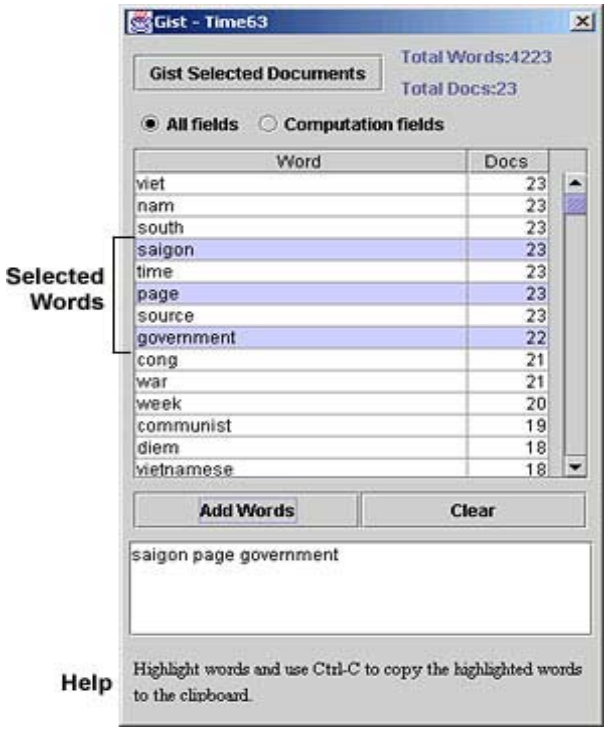

Figure 9: IN-SPIRE Gist Tool Display

Spearman's Rank Test

The nonparametric correlation test developed by Charles Spearman compares two independent random variables to determine if a correlation exists. Unlike other correlation tools, Spearman's rank test works with data that is ranked relative to the entire set of data for each variable. Spearman's rank correlation coefficient, represented as "r_s," provides a measure of correlation between each variable's ranked datasets. The formula for this measure of correlation is:

$$r_s = \frac{SS_{uv}}{\sqrt{SS_{uu} SS_{vv}}}$$

where

$$SS_{uv} = \sum (u_i - \bar{u})(v_i - \bar{v}) = \sum u_i v_i - \frac{(\sum u_i)(\sum v_i)}{n}$$

$$SS_{uu} = \sum (u_i - \bar{u})^2 = \sum u_i^2 - \frac{(\sum u_i)^2}{n}$$

$$SS_{vv} = \sum (v_i - \bar{v})^2 = \sum v_i^2 - \frac{(\sum v_i)^2}{n}$$

u_i = Rank of the *i*th observation in sample 1

v_i = Rank of the *i*th observation in sample 2

n = Number of pairs of observations (number of observation in each sample)

A shortcut can be used to approximate r_s when the number of ties in rankings for each sample is small compared to n. The shortcut formula is given below:

$$r_s = 1 - \frac{6\sum d^2}{n(n^2 - 1)}$$

where

$d_i = u_i - v_i$ (difference in the ranks of the *i*th observation for samples 1 and 2)

Using the shortcut formula it is easy to see when the rankings are identical the differences between the ranks will be zero (note: the example below uses n=10 for demonstration purposes only):

$$r_s = 1 - \frac{6\sum d^2}{n(n^2 - 1)} = 1 - \frac{6\sum 0^2}{10(10^2 - 1)} = 1 - 0 = 1$$

Therefore a perfect positive correlation between sample sets of ranks is characterized by a correlation coefficient of $r_s = 1$. When the ranks indicate perfect disagreement the result is $r_s = -1$, or perfect negative correlation.

The concept of correlation implies that two responses are obtained for each experimental unit. Rank correlation methods can be used to measure the correlation

between any pair of variables regardless of the difference in measurements in the two datasets. If two variables are measured on each of n experimental units, we rank the measurements associated with each variable separately. When ties in rankings for each sample set are found, each data point is given a value based on the average of the ranks they would receive if they were unequal but occurred in successive order. For example, if the 12^{th} through 15^{th} ranked measurements are tied each measurement will receive a rank of (12+13+14+15)/4 = 13.75. After this is done we calculate the value of r_s for the two rankings. This value measures the rank correlation between the two variables.

A two tailed test for Spearman's Nonparametric Test for Rank Correlation includes a null hypothesis that there is no correlation between the two sample populations being compared and an alternate hypothesis that a correlation does exist:

$$H_0: \rho = 0 \qquad \text{(Null Hypothesis)}$$

$$H_a: \rho \neq 0 \qquad \text{(Alternate Hypothesis)}$$

The value r_s, the sample rank correlation, is the test statistics. The rejection region is defined as $|r_s| > r_{s,\alpha/2}$ where the value of $r_{s,\alpha/2}$ is determined through the use of the t-statistic when the number of paired observations is greater then 30. The equation used to determine the test statistic, r_s, for $\alpha/2$ and n pairs of observations using the t-statistic is given below.

$$r_s = \sqrt{\frac{t^2}{t^2 + n - 2}}$$

The assumptions required for using Spearman's rank correlation are:

1. Randomly selected sample of experimental units for each of the two variables being measured

2. Continuous probability distribution of the two variables being measured.

Variable Definitions

This section discusses the dependent and independent variables involved in the research. Given the nature of this research, some leeway is required when assessing reliability and validity. Mainly, both variables were taken from existing databases instead of a designed experiment. Therefore, the data includes information that is irrelevant which may conceal potentially significant results.

Dependent Variable

The dependent variable for this study is the number of incidents per week for the six categories of incidents maintained in the JBS database. The definitions for each of the categories are described earlier in Chapter II. The number of incidents is easily determined from viewing the data separated by date and category in a Microsoft Excel spreadsheet. Category VIII (other) incidents could have been added to category VI (probe or scan) data for this research because category VIII incidents are usually later reclassified as category 6 (Svetlev, 2004). However, to ensure as high a level of validity as possible the combination of category VIII incidents is not done for this research.

The incident data is grouped by the number of incidents per week where each week starts on a Sunday and ends on a Saturday. The first week started on the first Sunday of January 2002 and ended on the last Saturday of June 2004. Weeks are used instead of days to account for any lag in dates assigned to each incident as well as other potential variability in the sets of data. Also, using the more numerous weekly data helps to comply with the Spearman's Rank correlation assumption of continuous data.

Independent Variable

The independent test group variable is the number of foreign news media reports per week with U.S. military content for each of the eight regions of the world monitored by FBIS. The independent control group variable is the total number of foreign news media reports per week for each of the eight regions of the world monitored by FBIS. The terms used in the query to identify and separate media reports with U.S. military content are extensive but not all inclusive. The news media report data are grouped by week in the same manner as the incident data to minimize possible lapses in the time to produce reports when compared to incident data and other potential variability within the sets of data.

Test Development

The null hypothesis (H_o) this research proposes is: no relationship exists between the number of foreign news media reports covering military events and network incidents against DoD systems. The alternative hypothesis (H_a) this research will either reject or fail to reject is: a relationship does exist between foreign news media reports covering military events and network incidents against DoD systems. The acceptable probability the null will be rejected when it should not, a type I error or α, is usually at or below 0.01. This means that if an α=0.01 is used then 1 out of 100 tests should be expected to result in a rejection of the null when the null hypothesis is true. Because there are almost 2500 individual tests performed for this research an α of 0.01 or higher would make the possibility of a type I error too great. Therefore an α of 0.001 is a more reasonable figure for this research making it unlikely for a significant amount of type I errors to occur.

Research Questions

What is the nature of the relationship between foreign news media reports covering military events and network incidents against DoD networks?

Investigative Questions

To better answer the research question, this research proposes to answer the following investigative questions:

1. Do statistically significant correlations exist between different foreign regions of news media reports involving U.S. military events and different categories of DoD network incidents?
2. During what timeframes do the most statistically significant correlations occur?
3. What is the content of the news media reports for the timeframes that are most significantly correlated?

Correlation Analysis

A correlation test requires each dataset to be quantitative, therefore the FBIS data needs to be converted into a quantitative form. The IN-SPIRE tool is able to enumerate the number of media reports by date using the Time Slicer function. This feature quantifies the news media data by enumerating the number of media reports occurring for each day of the two and a half year span. The Time Slicer tool will also be used in conjunction with the Query tool to enumerate the number of foreign news reports that contain military events for each day of the study. A conceptual analysis is done with the Query tool with the following list of terms to identify documents related in some way to

the U.S. military:

> "us military" or "u.s. military" or "usa military" or "u.s.a. military" or "united states military" or "us air force" or "u.s. air force" or "usa air force" or "u.s.a. air force" or "united states air force" or "us navy" or "u.s. navy" or "usa navy" or "u.s.a. navy" or "united states navy" or "us marines" or "u.s. marines" or "usa marines" or "u.s.a. marines" or "united states marines" or "us army" or "u.s. army" or "usa army" or "u.s.a. army" or "united states army" or "us dod" or "u.s. dod" or "usa dod" or "u.s.a. dod" or "united states dod"

The documents found to have military content can then be exported to create a sub-set of media reports. Again the Time Slicer tool is used to enumerate the number of media reports with U.S. military content for each day of the 30 month span. Both the daily news media and incident data sets are transformed into weekly data. The weekly timeframe is used to take into account the variability created by delays in publishing and correctly incident recording. All data, the number of incidents and media reports per week, are consolidated into a single Excel worksheet for visual analysis.

Several statistical software programs are capable of handling the requirements of this research; JMP 5.1 was the most readily available. The weekly incident data along with the weekly news media data are transferred into JMP 5.1 from the Microsoft Excel spreadsheet. The first tests are accomplished using the entire 30 months worth of weekly data. JMP 5.1 is used to perform a Spearman's Rho nonparametric rank test using multivariate analysis for each of the six categories of incidents against each of the eight regions of media reports and the eight regions of media reports with military content for a total of 96 tests.

The correlation tests between all foreign news media reports, regardless of military content, will be used as a test group. A comparison of the correlation results

between the news reports that did and did not reference the U.S. military will provide insight into whether or not the news media's coverage of military events has a more significant correlation then media reports in general.

Next, a time series test of the weekly data will be analyzed for each set of consecutive six month timeframes for the 30 months of data. There are 25 six month timeframes for a total of another 2400 tests altogether. JMP 5.1 will be used to perform a Spearman's Rho nonparametric rank test using multivariate analysis for each of the 25 six month datasets comparing the six categories of incidents against each of the eight regions of media reports and the eight regions of media reports with military content. The results of the time series test will be compared with the overall correlation tests to determine which correlations vary over time and by how much those correlations vary compared to previous test results.

Finally, the IN-SPIRE Gist tool will be used to perform exploratory analyses and find commonly used terms in the media reports for each month of the study by region. The Gist tool will "get the gist" of a collection of documents used in a dataset by listing the words commonly used between documents, ordered by the number of documents each word is referenced in. IN-SPIRE also displays the number of documents each word is found in. The terms found in the Gists of the entire 30 month period will be done for each region for analysis and to use as a baseline to compare against common terms found in each six month timeframe.

Due to computer speed and IN-SPIRE software limitations the media data could only be analyzed one months and region at a time, so it was necessary to perform two

successive Gists, as will be described below, to produce a list of common terms rather then a preferable single Gist. Furthermore, several insignificant terms will have to be added to the Stopword list to eliminate erroneous terms from the analysis. The additional Stopwords will be determined by finding common terms from a few random month/region document sets. Non key terms, such as adjectives or verbs, will be manually selected for inclusion into the Stopword list. Once a list is created it will be used for each analysis of news media reports.

A Gist of each month and region combination will be used to collect words common to at least 90% of the documents for that month and region. The terms will then be used to create a document of common terms for each month of each region. The result will be 30 documents of common terms for each region, for both all inclusive media reports and media reports covering the U.S. military, 480 documents altogether. The documents of common terms can then be viewed with IN-SPIRE for the entire 30 months of this study by region. At this point a regional Gist will be used to find the 20 most common words are in all 30 months of data for each region. The 20 common terms do not have to be common between every month, but the greatest number of months. The result is a regional list of 20 terms common to at least 90% of the documents for each month and region and common to the majority of months of that region.

A similar process is accomplished on only the months and regions found to have a significant correlation using the six month timeframe Spearman's Rank tests. The same documents created above of 90% common terms are viewed with IN-SPIRE for each set of months, by region, where a correlation was found to be significant in the 6 month

timeframe analysis. The significantly correlated timeframes for a region will be combined when they run in succession, are correlated to the same incident category, and have the same type of correlation (positive or negative). Again, the second set of common terms will be limited to the 20 most common key words for each set of months and regions found to be significantly correlated to DoD network incidents. A manual comparison between the 20 word lists and 30 month lists of key terms will be used to better understand potential reasons for any significant correlations.

IV. Analysis and Results

Chapter Overview

The purpose of this research is to determine what relationships exist between foreign media coverage of military events and DoD network incidents through qualitative codification and quantitative statistical analysis of data collected by NetDefense and the Foreign Broadcast Information System (FBIS). This chapter presents the results of the statistical and qualitative analysis to answer the three investigative questions described in Chapter III. The results of the three research questions are presented in their own sections below.

30 Month Timeframe Spearman Rho Tests

Based on a significance level of 0.001 and the 129 weeks of data, the rejection criterion was to reject the null hypothesis if $|r_s|>0.2867$. The results of the individual Spearman tests have been tabulated and are displayed in Table 2 and 3 below. These results indicate the null hypothesis should be rejected for a α of 0.001 in a two tailed test.

In all, 10 of the 96 rank correlations were determined to be statistically significant with a significance level of 0.001. Six of the ten significant correlations involved media related to military events. The average value of the six significant correlations between network incidents and military related media, 0.4318, was larger then the average r value of the other four correlations of all inclusive media, 0.3631.

Of the six types of the incident categories studied for the full 30 months, III, VI, and VII (attempted access, probe or scan, and malicious code respectively), were found to have at least one significant correlation. In addition, three of the eight regions for all

inclusive media reports had at least one significant correlation: China, East Europe, and Sub-Saharan Africa. Five regions for U.S. military related media reports had at least one significant correlation: Central Eurasia, East Asia, East Europe, Near East and South Asia, and West Europe. Both positive and negative correlations were found to be significant in the results of the rank tests. With the exception of category VII incidents for all inclusive media, each region or category maintained either positive or negative correlations. Negative correlations were more common with six being negative and four being positive.

Table 4: Results of Spearman Rho Test for Each Region and DoD Network Incident Combination for All Media Reports from Jan 2002 Through Jun 2004

	I	II	III	IV	VI	VII
Central Eurasia	-0.1216	0.1309	-0.0667	-0.0012	-0.0023	-0.1849
China	0.1702	0.0116	0.1201	-0.1559	-0.1760	0.3325*
East Asia	-0.0537	0.0291	0.0456	0.0973	-0.1530	-0.1083
East Europe	-0.0420	-0.0191	-0.4355*	0.1596	0.0382	-0.2783
Near East/South Asia	0.0319	-0.0159	0.0497	-0.0984	-0.2759	0.0606
Sub-Saharan Africa	-0.2524	0.1689	-0.3498*	0.2095	-0.1980	-0.3345*
The Americas	-0.0611	-0.0802	0.1919	-0.0544	-0.0653	0.0823
West Europe	0.0975	-0.0383	0.0478	-0.0090	0.1292	0.0082

* r_s values greater than the critical value 0.2865 at the 0.001 level for a two tailed test

Table 5: Results of Spearman Rho Test for Each Region and DoD Network Incident Combination for Military Media Reports from Jan 2002 Through Jun 2004

	I	II	III	IV	VI	VII
Central Eurasia	-0.2848	0.1467	-0.2502	0.1561	-0.0618	-0.5124*
China	-0.0583	0.0560	0.1281	0.0634	-0.2089	-0.1990
East Asia	-0.0561	0.1012	0.0215	0.1211	-0.3143*	-0.3153*
East Europe	-0.1678	-0.0381	0.4535*	-0.0137	-0.0164	0.1381
Near East/South Asia	-0.0436	0.0983	0.4753*	-0.0870	-0.0433	0.1415
Sub-Saharan Africa	-0.1135	-0.0780	0.0652	-0.0144	-0.0848	0.0352
The Americas	-0.0427	0.0511	0.1150	-0.0152	-0.1057	-0.2137
West Europe	0.0059	0.0895	0.5198*	0.0025	0.0456	0.2058

* r_s values greater than the critical value 0.2865 at the 0.001 level for a two tailed test

6 Month Timeframe Spearman Rho Tests

Based on a significance level of 0.001 and the 26 weeks of data for each six month correlation test, the rejection criterion was to reject the null hypothesis if $|r_s|>0.6034$. The 2400 tests conducted for this part of the research made it inconvenient to list the results of each test. Therefore, the results of the individual Spearman's Rho tests have been consolidated in Table 4 and 5 below to list each significant correlation coefficient found and the months, region, and incident category in which it was significant. None of the media-incident correlations other then those listed in table 4 and 5 for the six month timeframes exceeded the minimum r_s value of 0.6034 and are therefore not listed in Tables 4 and 5 below. These results indicate the null hypothesis should be rejected for a α of 0.001 in a two tailed test.

In all, 39 of the 2400 rank correlations were determined to be statistically significant with a significance level of 0.001. 28 of the 39 significant correlations existed within media related to military events. Much like the 30 month correlations, the average value of the 28 significant correlations between network incidents and military related media, 0.6654, was slightly larger then the average r value of the other 11 all inclusive media incident correlations, 0.6513.

Of the six types of incident categories studied for the six month timeframes, I, III, VI, and VII (unauthorized root access, attempted access, probe or scan, and malicious code respectively), were found to have at least one significant correlation. In addition, every region but West Europe was found to have a significant correlation using all inclusive media reports. However, every region but East Asia and The Americas were

found to have a significant correlation using news media reports covering the U.S. military. Both positive and negative correlations were found to be significant in the results of the rank tests. With the exception of category III incidents for military related media correlations in Central Eurasia, each region and incident category correlation maintained either positive or negative correlations. Unlike the 30 month tests, positive correlations were slightly more common with 24 significant correlations being positive and 15 negative ones.

Table 6: Results of Spearman Rho Test for Each Region and DoD Network Incident Combination for All Media Reports from Jan 2002 Through Jun 2004 in Six Month Increments

Cat	Region	r_s	Months
I	East Asia	0.6035	1-6
	Sub-Saharan Africa	-0.6112	19-24
III	China	-0.6192	3-8
	Sub-Saharan Africa	0.633	4-9
	The Americas	-0.6101	4-9
VI	East Europe	0.6595	17-22
	East Europe	0.6194	18-23
	East Europe	0.6808	25-30
	Near East & South Asia	-0.6923	3-8
	The Americas	0.7492	25-30
VII	Central Eurasia	0.6857	23-28

Table 7: Results of Spearman Rho Test for Each Region and DoD Network Incident Combination for Military Media Reports from Jan 2002 Through Jun 2004 in Six Month Increments

Cat	Region	r_s	Months
I	Central Eurasia	-0.6344	22-27
	Central Eurasia	-0.6467	23-28
	Central Eurasia	-0.6661	24-29
	Sub-Saharan Africa	-0.644	16-21
	Sub-Saharan Africa	-0.6315	17-22
	Sub-Saharan Africa	-0.6801	18-23
	Sub-Saharan Africa	-0.6312	19-24
III	Central Eurasia	-0.8299	7-12
	Central Eurasia	-0.6903	8-13
	Central Eurasia	0.7917	14-19
	Central Eurasia	0.7172	15-20
	China	0.6207	10-15
	China	0.658	14-19
	China	0.7109	15-20
	East Europe	0.6161	10-15
	Near East & South Asia	0.7165	4-9
	Near East & South Asia	0.7223	5-10
	Near East & South Asia	0.6152	10-15
	West Europe	0.6509	4-9
	West Europe	0.6358	5-10
	West Europe	0.6675	10-15
	West Europe	0.6662	11-16
	West Europe	0.6264	12-17
	West Europe	0.6377	13-18
	West Europe	0.6411	14-19
VII	Central Eurasia	-0.6059	24-29
	East Europe	-0.6641	17-22
	Near East & South Asia	0.6119	21-26

Significant Media Content

The results found in the content of the foreign media reports were divided into

two sections. The first section is concerned with the words most significant to each region for all 30 months. The second section displays the 20 most significant key terms for those months and regions found to have the highest correlation significance.

Regional Exploratory Analysis

A list of Stopwords (Appendix A) was extracted from three test Gists using the data from three randomly selected sets of news media reports: January 2002 Central Eurasia, July 2002 China, and March 2004 The Americas. These reports were combined and used to manually extract words insignificant to the intent of this research not already included in the IN-SPIRE Stopword list. These words were then added to the existing IN-SPIRE Stopword list.

Next a Gist was performed to determine what words were common to at least 90% of the media reports for a given month and region. This list was then used to determine what words, from the lists of terms common to at least 90% of media reports, were most common to all 30 months of media reports for each region. The number of most common terms was limited to 20 to simplify a manual review. Each of the 20 words on a list was in at least 90% of the media reports for a given month and region, and also one of the top 20 most commonly used key terms between those months for the region. The resultant lists are shown in Table 6 and 7 below. Each list is ranked first by frequency then alphabetically, so the most frequently used terms are first on the list in alphabetical order and followed by the second most frequently used terms in a separate alphabetical order.

Through manual review of Table 6 and 7 the common terms suggest the primary

content of each region's media are concerned with places within the region, politics, and government. A few words which relate to the research being performed, such as "internet", "army", "terrorism", and "weapons" are present but do not appear to be any more relevant to correlated regions then non-correlated regions.

Table 8: Results of the Media Content Analysis for All Media Reports from Jan 2002 through Jun 2004

Central Eurasia*	China	East Asia*	East Europe*	Near East & South Asia*	Sub-Saharan Africa*	The Americas	West Europe*
cooperation	audiences	computer	belgrade	economic	democratic	economic	english
economic	beijing	domestic	democratic	english	economic	english	foreign
english	chinese	economic	english	foreign	english	foreign	internet
foreign	economic	editorial	european	internet	foreign	internet	minister
leader	english	english	foreign	leader	french	minister	national
minister	filing	foreign	minister	minister	internet	national	policy
ministry	foreign	internet	ministry	national	leader	officials	political
moscow	hong	intervention	national	political	minister	political	president
national	internet	japan	political	president	national	president	security
political	kong	korea	president	security	opposition	security	united
president	national	minister	republic	war	political	spanish	european
russia	prc	national	security	arabic	president	united	french
security	president	officials	social	iran	security	trade	paris
authorities	root	president	union	islamic	war	million	turkey
relations	taiwan	rok	law	officials	officials	american	union
vladimir	xinhua	seoul	opposition	policy	republic	policy	economic
law	minister	tokyo	economic	united	united	ministry	german
republic	officials	ministry	leader	arab	police	social	leader
federal	political	united	internet	israel	talks	leaders	democratic
itar	united	yonhap	police	israeli	nation	police	war

* Regions found to have at least one significant correlation

Table 9: Results of the Media Content Analysis for Media Reports with Military Content from Jan 2002 through Jun 2004

Central Eurasia*	China	East Asia*	East Europe*	Near East & South Asia*	Sub-Saharan Africa*	The Americas	West Europe*
moscow	beijing	english	english	english	president	english	bush
russian	chinese	internet	minister	foreign	english	foreign	foreign
defense	defense	japan	political	internet	african	internet	minister
political	english	tokyo	war	iraq	internet	president	president
president	force	united	army	minister	minister	united	security
security	foreign	defense	defense	political	national	minister	united
united	internet	foreign	european	president	united	national	war
force	national	intervention	foreign	security	american	security	washington
foreign	political	korea	national	united	army	war	internet
minister	prc	national	nato	war	war	washington	iraq
american	president	war	president	bush	french	political	political
ministry	security	korean	security	force	security	army	french
war	united	officials	united	islamic	force	bush	national
army	war	security	force	american	iraq	force	force
cooperation	weapons	computer	ministry	afghanistan	foreign	troops	policy
national	bush	president	troops	army	kenya	officials	army
armed	economic	troops	iraq	policy	armed	spanish	english
relations	policy	rok	commentary	washington	terrorism	defense	american
territory	iraq	force	policy	arab	bush	iraq	iraqi
english	power	minister	internet	iraqi	political	terrorism	weapons

* Regions found to have at least one significant correlation

Significant Timeframe Exploratory Analysis

There were 2400 individual tests given the two sets of media reports for 8 regions, 6 incident categories, and 25 six-month timeframes. Below in tables 8 and 9 are the results of the media content analysis for the months out of these 2400 tests found to be significant. Each list contains 20 of the most commonly used key terms for a given region and incident category during the months significant correlations were found. The lists were compiled in a similar manner to the regional exploratory analysis above and are described in Chapter III. Some of the timeframes were combined with one another because they ran concurrently and had the same positive or negative correlation. When this was the case, the most common key terms were found for the combination of months found to be correlated. Because of this method the 39 correlations found for the six-month timeframes were consolidated into 21 correlations. Each of the 20 words on a list

was in at least 90% of the media reports for a given month and region, and also one of the top 20 most commonly used key terms between those months and regions. Each list is ranked first by frequency then alphabetically, so the most frequently used terms are first on the list in alphabetical order and followed by the second most frequently used terms in a separate alphabetical order.

The lists were manually reviewed for their content and compared to the regional media content lists in Table 6 and 7 above. No significant terms were distinguished from the lists in Table 8 and 9 below from the lists in Table 6 and 7 above. In the lists of Table 8 and 9 below a few unique terms were identified, but were not consistent throughout the lists.

Table 10: Results of the Six Month Timeframe Media Content Analysis for All Media Reports from Jan 2002 through Jun 2004

Category I		**Category III**			**Category VI**				**Category VII**
East Asia	Sub-Saharan Africa	China	Sub-Saharan Africa	The Americas	East Europe (Weeks 17-23)	East Europe (Weeks 25-30)	Near East & South Asia	The Americas	Central Eurasia
computer	african	audiences	african	economic	democratic	democratic	arab	administration	economic
disseminated	democratic	beijing	democratic	editorial	economic	economic	arabic	american	foreign
domestic	economic	chinese	foreign	foreign	european	european	foreign	economic	minister
editorial	foreign	economic	french	internet	foreign	foreign	internet	foreign	moscow
foreign	french	filing	internet	minister	law	headline	islamic	internet	national
internet	internet	foreign	leader	national	minister	minister	israel	minister	political
intervention	leader	hong	minister	officials	ministry	ministry	israeli	national	president
japan	leaders	internet	national	political	national	national	leader	political	russia
japanese	minister	kong	officials	president	political	political	minister	president	russian
korea	national	national	political	security	president	president	national	security	leader
largest	political	political	president	spanish	reference	reference	palestinian	spanish	ministry
minister	president	prc	security	united	serbia	republic	political	united	authorities
national	security	president	web	administration	serbian	security	president	leader	itar
president	war	root	leaders	colombia	union	serbian	security	officials	law
rok	opposition	taiwan	opposition	american	belgrade	union	united	trade	putin
selected	privately	xinhua	talks	million	internet	police	war	million	relations
seoul	kenya	minister	war	economy	opposition	serbia	iran	ministry	security
tokyo	nation	officials	economic	financial	republic	social	officials	police	vladimir
korean	power	trade	united	law	police	election	india	policy	cooperation
officials	talks	cooperation	police	policy	security	belgrade	pakistan	efe	election

Table 11: Results of the Six Month Timeframe Media Content Analysis for Media Reports with Military Content from Jan 2002 through Jun 2004

Category I		**Category III**						**Category VII**		
Central Eurasia	Sub-Saharan Africa	Central Eurasia (Pos Corr)	Central Eurasia (Neg Corr)	China	East Europe	Near East & South Asia	West Europe	Central Eurasia	East Europe	Near East & South Asia
russia	president	defense	american	beijing	army	foreign	internet	russia	army	army
defense	united	force	defense	chinese	foreign	internet	president	defense	commentary	foreign
foreign	american	foreign	foreign	defense	iraq	minister	security	foreign	defense	internet
moscow	internet	iraq	minister	force	minister	political	united	moscow	foreign	iraq
political	national	minister	ministry	foreign	national	president	war	political	iraq	iraqi
russian	war	ministry	moscow	internet	political	security	foreign	russian	minister	minister
security	african	moscow	political	political	security	united	iraq	security	nato	president
united	army	political	president	prc	united	war	minister	united	political	security
american	force	president	russia	president	war	afghanistan	bush	american	president	troops
armed	french	russia	russian	security	defense	american	european	armed	united	united
bases	security	russian	security	united	force	bush	french	bases	war	war
cooperation	bush	security	united	war	nato	iraq	political	cooperation	european	afghanistan
minister	iraq	united	cooperation	weapons	president	washington	washington	minister	bulgaria	american
president	minister	american	national	economic	european	afghanistan	force	ministry	ministry	attacks
iraq	nation	war	army	iraq	ministry	american	german	president	national	baghdad
ministry	economic	national	force	national	reference	bush	national	iraq	reference	force
americans	kenya	relations	iraq	bush	republic	iraq	defense	nato	security	killed
force	liberia	weapons	nato	power	internet	washington	policy	war	washington	policy
national	nairobi	americans	armed	troops	iraqi	arab	saddam	americans	bulgarian	political
nato	nigeria	armed	english	nations	un	policy	weapons	army	citizens	soldiers

V. Conclusions and Recommendations

Conclusions of Research

This study performs both quantitative and qualitative analysis on a collection of 30 months worth of foreign news media reports from over 3,000 international sources divided into eight separate regions, excluding the United States. The analysis was designed to determine if a correlation existed between foreign news media reports covering U.S. military events and network incidents against DoD networks. It also was meant to help better understand the nature of such a relationship by determining what key terms were used in the contents of the media reports found to be significantly correlated with the news media reports. Significant correlations were found between several combinations of regions and categories of network incidents for both news reports covering the U.S. military and the entire collection of news reports. However, a greater amount of more significant correlations were found when the news reports pertained to military events. To help understand the nature of the correlation the most common terms used within the thousands of foreign news reports were found. Unfortunately, the correlations were only moderate and the key terms only led to a slightly better understanding of such relationships. Therefore a correlation does exist, but a determination of causation is left unanswered.

Review of Results

It is obvious a great deal more analysis is required to determine the true nature of the relationship between foreign news media reports and DoD network incidents. The three investigative questions were answered, but resulted in more questions then answers.

The following sections review the results from the two types of tests conducted in this research.

Correlation Tests

Clearly the data are not in complete agreement when we look at the results in the differences between the six month timeframes and the regional analysis. I expected any significant regional correlations for a region and incident category to contain a large number of six month correlations for the same region and incident category. However, only a few such cases existed. For military coverage report data there were three cases were significant correlations existed between both the 30 and the 6 month analysis. Only one case was found with all inclusive news data. In all cases the number of months found to be significant through the six month tests did not correlate with the magnitude of the correlation coefficient, at least not relative to each other. For example, Sub-Saharan Africa news reports were found to be correlated with category III incidents positively for the 30 month test and negatively for a six month correlation test. In addition, the number and magnitude of six month correlations were much higher for the Near East & South Asia region then the Central Eurasia region, but the 30 month correlation for Central Eurasia was higher.

The validity of the decision to reject the null is improved when the total numbers of correlations are examined in light of the significance level. I expected to see two or three coefficients within the rejection region because the significance level was 0.001 and there were 2496 test. This means about 2.5 tests should be the result of a Type I error. In all, 49 tests resulted in a rejection of the null far exceeding the bounds of what may put

the decision to reject the null in question.

Looking back at the data the number of news media reports covering U.S. military events per week for East Europe, Sub-Saharan Africa, and The Americas were quit low and probably not suitable for rank correlation testing. Furthermore, the same case can be made for the number of category I, II, and IV network incidents per week. This is especially the case for category IV incidents were a large amount of zero values created an especially high number of ties in ranking the data. Fortunately few correlations were found to be significant involving the questionable data.

Media Content

The content of the news media reports were mostly of a political nature. There were also several specific places of high interest which coincided with the region of media reports. A few key words did stick out from the lists such as “internet”, “army”, “weapons”, and “terrorism” but do not appear to be relevant to the nature of a correlation. No consistent set of key words were found which might lead to a better understanding of the cause of a correlation. The most significant finding, when looking at the results of the news media content analysis, is the need for further refinement in how the exploratory analyses are conducted.

Practical Implications

The significance of this research is not only how a correlation was shown to exist between foreign news media coverage of U.S. military actions, but how most of the correlations found were with Category III incidents (attempted access). Category III incidents are one of the most prevalent types of incident, which is not surprising as it is

the most simplistic for an attacker to perform and get away with. The key issue with this type of attack is how it is used as a way to scope out a network's defenses. Attempts at access are the first step in attaining access to a network and is therefore more likely to be conducted in the same timeframe as a media report which is correlated with it. I am most concerned with the lack of effective IDS in which case the true number of successful attacks isn't being recorded and a significant correlation may go unnoticed. However, this is only a slight concern given this test was based on ranking the data. Even if there were a significant number of successful attacks going unnoticed the relative nature of the tests should have shown a significant correlation if one existed.

Because no direct causation could be determined, no actions can be made by the DoD to better their defenses against network incidents. Once follow-on research is accomplished and quantifies what the aspects of the DoD and foreign news media relationships are, more direct actions can be specified to minimize network attacks.

Recommendations

This study was an expansion of previous research into how news media can be used to better predict or defend against future network incidents. The amount of previous research was small and its content was vague and based on somewhat erratic data. There are multiple areas in this field of study for expansion and improvement.

News Media and Network Incident Relationship

The most notable recommendation is to narrow the focus of the news media content from all inclusive and U.S. military coverage to several mutually exclusive yet collectively exhaustive types of news content. The fact that significant correlations were

found shows a relationship does exist between foreign news media and DoD network incidents and should be explored further. A higher significance level was found in the correlation coefficient with tests of foreign news media reports containing U.S. military events then tests involving all inclusive foreign news media reports. This difference shows how the separation of media reports containing military events has proportionately more significantly correlated media reports then the entire collection of news media reports.

Another consideration is the potential lag between published reports and incident reporting and categorization. The same data could be reanalyzed taking into account lags by matching incident data from each week with the previous week of media data, or vise versa. Such tests would show how time affects the relationship. The lag tests could also be used as evidence to support or refute theories of causation.

Looking at the moderate magnitude of the correlations, using the most common key terms within the news reports was perhaps misleading. The true nature of a correlation was much less common. A better way to go about the analysis would have been to use IN-SPIRE, or a better data mining tool, to quantify the less frequently used terms then use this list of terms to separate the media into meaningful yet separate sections for analysis. A few suggested types of media content more specific to a relationship are: forms of conflict, political viewpoints, methods of network attacks, incident related news, and computer related news. Using this improved analysis technique the relationship could then be further reduced to its true nature and justify reason for a causal-comparative study to be performed.

One last idea is to perform a more detailed correlation analysis by separating the different DoD agencies network incidents. Such a study may show how an agency is being singled out for attacks, or how certain news media is correlated more to certain DoD agencies. This may, however, prove difficult with limited incident data.

Text Mining

The techniques used to extract the news media content in this research were less then ideal. The obvious solution would be to gain access to more powerful data mining tools and computer systems. If this is the case, then it may be possible to view more then a couple months' worth of media reports for a single region at a time. To be able to view the set of reports as a whole would drastically improve the ability to determine how to divide the media into separate meaningful sections. In the absence of such tools, one can learn from the techniques used in this research.

The Stopwords tool was necessary while using IN-SPIRE software to remove an abundance of insignificant words cluttering the list of key terms found for a set of reports. Several stopword lists could be combined from the months of reports to eliminate the insignificant information and improve the results of the Gist tool. A thorough use of these tools to find less significant key words may prove beneficial when separating a set of documents into separate yet all inclusive sections.

Appendix A

Additional Stopwords used for Media Content Analysis:

unclassified report prohibited material owners permission contain copyright fbis dissemination copying copyrighted jan feb mar apr may jun jul aug sep oct nov dec text gmt translated source description January February March April May June July august September October November December agency government news information main time told people according country transcribed deputy head situation www affairs service independent international newspaper including countries official meeting press correspondent excerpt provided company region forces means chief development council special interfax office former omitted set held visit world decision website passage department support day version local central tv following television media reports received prime level issue site system presenter devoted district daily operation article signed course party representatives control similar issues result regional agreement results reported called question cent data staff radio current major noted percent discussed director yesterday opinion taking five avn written position intended past days recently process conditions measures prior help interview ago believe air example times plans particular various total start discuss near basis experts organization left purposes speaking actions months session content increase services found serious expected organizations based stressed carried period operations city companies consent decided market secretary reason announced recent soon term six activities believes life paper anti controlled redistribution centre plan view close started programme change difficult reserved half line week holding entitled real planned html sent isp expressly republication currently channel north ready units equipment expressed representative

sources events statement involved efforts video hold building addition attention station documents terms due meet aimed technical center industry created officers house stated met matter third considered role assembly words prepared added details deputies aid regions adopted mass seen simply hand internal parties changes document earlier amount questions form leave led reached action moreover Wednesday Monday Tuesday Thursday Friday Saturday Sunday especially saying increased beginning entire paid hope bilateral activity despite status personnel using approved true resources return effect brought draft interior remain sector single pro field possibility private month program create connection confirmed premier bodies list provide audience owned live southern established managed spokesman account moment agencies final project speaker arrived receive decisions heads specialists trying plant stock free accordance agreed seven reach reasons name previous person step top board deal natural experience potential specific active scale ensure views immediately organized issued participation sign carrying majority conducted talk settlement developing exchange regard headquarters task complex facilities assistance act implementation training whom carry consider community agree develop reform stage laws executive meetings march figures passed appointed influence resolution investment presence positive closed bring rate understand property agreements idea concerned east discussion demand planning prospects particularly cut registered hours happened growth mean completely remains common leading base headed date space structures run late peace participants coming movement look supreme supply changed viewpoint ties nor operating land developed health lost included industrial northern probably proposed meanwhile declared purpose call concern concerning charge commercial systems towards hard subject respect billion join elite

event allow speak opportunity makes projects begin rule supported personal finally positions submitted purchased team url vice town proposals significant effective lead pressure tasks completed detained regarding direct attempt try move talking language living additional figure cost progress stop creation launched include calls candidates acts highly structure intends eight ru west south importance worth note formed outside tried ones explained spent impossible described independence mutual incidentally complete located appeal key statements mission built continuing proposal responsible instance unit guard range comment decree existing accused begun extremely steps st via allowed forced informed customs directorate rise principle promised normal related intend responsibility

Bibliography

Allen, Julia, Alan Christie, William Fithen, John McHugh, Jed Pickel, Ed Stoner. *State of the Practice of Intrusion Detection Technologies*, Contract C-F1962895-C-0003. Pittsburgh PA: Carnegie Mellon University Software Engineering Institute. January 2000 (CMU/SEI-99-TR-28).

Aukofer, Frank and William P. Lawrence. "America's Team, the Odd Couple Report on the Relationship Between the Media and the Military." Nashville: The Freedom Forum first Amendment Center, 1995.

CERT/CC. "CERT/CC Overview." PowerPoint Presentation. CERT Coordination Center Software Engineering Institute Carnegie Mellon University, 2003.

Computer Fraud and Abuse Act of 1986.

Daigle, Richard C. "An Analysis of the Computer and Network Attack Taxonomy." MS Thesis, AFIT/GIR/ENV/01M-04. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2001 (ADA391250).

Department of Defense (DoD). *Clearance of DOD Information for Public Release*. DoD Directive 5230.9. Washington DC: GPO, Apr. 9,1996. http://sites.defenselink.mil.dd5230_9.html

Department of Defense (DoD). *Cooperation with U. S. News Media Representatives at the Scene of Military Accidents Occurring outside Military Installations*. DoD Directive 5419.14. Washington DC: GPO, Oct. 25, 1963. http://web7.whs.osd.mil/pdf/d541014p.pdf.

Department of Defense (DoD). *DoD Information Security Program.* DoD Directive 5200.1. Washington DC: GPO, December 13, 1996.

Department of Defense (DoD). *Information Security Program Regulation*. DoD Directive 5200.1-R Washington DC: GPO, January 1997.

Department of Defense (DoD). *Department of Defense Information technology Security Certification and Accreditation Process (DITSCAP) Application Manual*. DoD Manual 8510.1-M. Washington DC: GPO, July 2000.

Department of Defense (DoD). *Support to Computer Network Defense (CND).* DoD Instruction 8530.2. Washington DC: GPO, March 9, 2001.

Gibbs, Mark, and Todd Brown. *Absolute Beginner's Guide to Networking* (2nd Edition). Indiana: Sams Publishing, a Division of Macmillan Computer Publishing, 1995.

Ginn, Patrick W. "Correlation Analysis of Fleet Information Warfare Center Network Incidents". Naval Postgraduate School. June 2001.

Hill, Raymond R., Jr. "The Future Military-Media Relationship: The Media as an Actor in War Execution." 1997.

Howard, John D. "An Analysis of Security Incidents on the Internet, 1989-1995, Ph.D. Dissertation, Department of Engineering and Public Policy/Carnegie Melon University, Pittsburgh, PA. 7 April 1997.

Howard, John D., and Thomas A. Longstaff. "A Common Language for Computer Security Incidents, October 1998 (SAND98-8667).

Joint Pub 3-13. Joint Doctrine for Information Operations. Oct. 9, 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

Joint Pub 3-53. Doctrine for Joint Psychological Operations. Sep. 5, 2003. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf.

Joint Pub 3-57. Doctrine for Joint Civil Affairs. Feb. 8, 2001. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_57.pdf.

Joint Pub 3-61. Doctrine for Public Affairs in Joint Operations. May 14, 1997. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_61.pdf.

Korzyk, Alexander Sr. "A Forecasting Model for Internet Security Attacks." National Information System Security Conference, 1998.

Lipson, Howard F. "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues." Carnegie Mellon University Software Engineering Institute. Nov 2002. Special Report CMU/SEI-2002-SR-009.

McHugh, James J. "The Media Factor: An Essential Ingredient to Operational Success." June 13, 1997.

McHugh, John. "Intrusion and Intrusion Detection." IJIS, 1: 14-35 (2001).

Moreau, René. *The Computer Comes of Age* (Original Title Ainsi naquit l'informatique). 1981 translated to English by The Massachusetts Institute of Technology. Massachusetts: The MIT Press, 1984.

National Information Infrastructure Protection Act.

Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD (C3I)) Memorandum, "The Defense Information Systems Security Program (DISSP)," August 19, 1992.

Snyder, John B. "Seeing Through the Conflict: Military-Media Relations." U.S. Army War College. Jul 2003.

Svetlev, Alex M. Interviews via e-mail correspondence. 10 Feb 2004 – 30 Aug 2004.

Witkin, Norman. *Enterprise Networking for Information Systems Professionals*. New York: Van Nostrand Reinhold, a division of International Thomson Publishing Inc, 1995.

Yurcik, William, David Loomis, and Alexander D. Korzyk, Sr., "Predicting Internet Attacks: On Developing An Effective Measurement Methodology," Proceedings of the 18th Annual International Communications Forecasting Conference. 1-9. Seattle: ICFC-2000

Vita

Capt Jason Dean Jaros was born on 25 January 1975 in Fridley, Minnesota. He graduated from Anoka Senior High School in Anoka, Minnesota in June 1993. He entered undergraduate studies at Mankato State University in Mankato, Minnesota where he graduated with a Bachelor of Science degree in Mechanical Engineering in June of 1997. He was commissioned through OTS program in November 1998.

His first assignment was as an ACE Lt at Altus AFB OK where he was assigned as a Deputy Information Systems Flight Commander, Plans Flight Commander, and Support Group Executive Officer. In January of 2001 he was given his second assignment to the 17th Test Squadron, Detachment 3, Patrick AFB FL. During his tour at Patrick AFB he conducted planning and testing of the Range Standardization and Automation program. In August 2003, he entered the Graduate Information Resource Management program, School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to the Resources Branch of the Plans, Programs and Resources Directorate, HQ USAFE/A6 Communications and Information Directorate, Ramstein AB, Germany.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
21-03-2005	Master's Thesis	Sep 2003 – Mar 2005

4. TITLE AND SUBTITLE
Determining a relationship between foreign news media reports covering U.S. military events and network incidents against DoD networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Jaros, Jason, D., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-08

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Defense University
IRM College
Attn: Lt Col Clifton Poole
Fort Lesley J. McNair
Washington, DC 20319-5066

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis explores the nature of the relationship between foreign news media and network incidents against DoD networks. A rank correlation was performed between the number of network incidents against DoD networks and foreign news media reports covering U.S. Military events. Further analysis was conducted to determine the key terms used in the contents of foreign news media reports for the months the reports were significantly correlated with network incidents. Several significant correlations were found between various combinations of regions and categories of network incidents. However, the correlations were only moderate and the key terms only led to a slightly better understanding of such relationships.

15. SUBJECT TERMS

Information Assurance, Information Security, Internet, Internet Security, Computer Security, Network Security, Information Operations, Statistical Analysis, Correlation Analysis, Content Analysis, News Media, Network Incidents

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			David D. Bouvin, Capt, USAF
U	U	U	UU	97	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4742 (David.Bouvin@afit.edu)