ABSTRACT

This paper discusses the use of steganography as a tool for hiding covert communications between terrorists. Steganography tools are being used within different mediums to conceal communications from one terrorist or terrorist cell to another without the knowledge of a third party. Terrorists use various steganography tools (either freeware or for purchase) to embed or "hide" data in a carrier file; commonly an image, audio, or video file. The tools have the ability to conceal information in a manner unnoticeable to the naked eye requiring further investigation and verification if suspected.

Through the use of steganography many countries are rising as greater threats to the United States within the cyber-realm. With the recent incidents involving the penetration of U.S. computer systems, knowledge of steganography tools and how it is used has become more relevant. Agencies need to gain a better understanding of the methods and tools that are being used by those posing the greatest threat to our national security while continuously improving upon existing policies and risk assessment measures; as well as training and educating all levels of employees to be more alert for possible steganographic messages.

THE USE OF STEGANOGRAPHY IN CYBER – TERRORIST COMMUNICATIONS

By

Kerry Ryerson Mildon

A Capstone Project Submitted to the Faculty of

Utica College

March 18, 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science Cybersecurity – Intelligence and Forensics

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

ACKNOWLEDGEMENTS

I would like to thank my husband Eric for always supporting me throughout my entire educational endeavors and sacrificing so much to provide for our family; thank you for serving our country. To my children Joshua and Kayla, thank you for always telling me “you will get an ‘A’ mommy, do not worry.”

To my sister Kim, nephew Javon, and brother-in-law Rob; you are true blessings in my life. I thank God that you are all together again and safely home. I thank you Rob for your service.

I would also like to thank Professor Randall K. Nichols for his assistance and guidance throughout my entire tenure at Utica College and especially throughout my Master’s program. I would like to thank Mr. Chester Hosmer. Your expertise and guidance throughout this adventure has been extremely appreciated.

Finally, I would like to thank my mother, Gail Ryerson, you may not be with me anymore, but in your way I know you were always by my side

STATEMENT OF PROBLEM

Terrorist cells have found new ways to communicate with one another (McCullagh, 2001). Recent studies have shown an increase in cyber-terrorism and use of steganography as a tool for communication between terrorists (McCullagh, 2001**).** ***The purpose of this research is to examine the rise of steganography as a communication method between terrorist groups in order to carry out terrorist acts against the United States.***

Research Questions

Steganography communication can be examined from different directions.

- What steganography tools are being used by terrorists to hide the communications?
- In what media do terrorists hide intelligence information and attack plans?
- What tools are available to find and "crack" steganographic messages?
- Does current DOD and Government security policy appropriately address steganography in terrorist communications? If not, what improvements are needed?

This paper examines methods and procedures used to find steganographic communications, analyze traffic networks, and develop reliable intelligence.

Evidence of Steganography in Cyber-Terrorism Communications

Steganography has been used for many years as a method of hidden or secretive communication. As stated in the previous section, steganography is the art of hiding data or information within a larger host file so it is not visible in plain view (SANS, 2001). According to Maura Conway (2008), USA Today reported in February 2000, that suspected terrorists were starting to use steganography for covert communications between cells to carry out missions. Until articles such as the USA Today article surfaced, steganography was considered the "poor cousin of cryptography" (Conway, 2008), meaning that steganography hides a message that has not been altered; whereas cryptography actually changes the original message into a new or jumbled message.

Terrorist cells have used cellular phones, simple e-mail messages, and even satellite phones. It is not the most secretive method of communication, but if used properly it can aid the suspect to elude authorities for a period of time (Gaudin, 2001). Some are still employing these methods, but with an increase in technological advancements and the ability to conceal information, many are finding new methods of communication (Gaudin, 2001).

In order to show that steganography is being used for communication one must first look at how steganography is used. For the most part steganography has been examined in an academic sense. Sayan Chakraborty (Radcliff, 2002), Vice President of Engineering at Sigaba Corporation was quoted as saying, "most people study steganography as an academic discipline or out of curiosity." Chakraborty went on to say that he, "does not know if even terrorist groups would actually use it" (Radcliff, 2002).

The evidence showing that steganography is used by terrorists is sparse. In one study, Professor Randall K. Nichols (2004) was able to show that Al Qaeda had capabilities of using "steganography with robust cryptography." Nichols found that although other studies found no evidence of steganographic messages, they used "bad targets" and did not "investigate spam e-mails and pornography" (Nichols, 2004). According to Professor Nichols (2004) it is not uncommon to find steganography messages in, “family pictures and e-mail inserts following religious beliefs.”

When the United States government was prosecuting suspects of the “1998 terrorist bombings of two U.S. embassies in Africa” many tried to show that some of the “top Al Qaeda officials lead two lives; one running a terrorist network and a second operating a business” (Gaudin, 2001, pg. 48). The business fronts that terrorist cells use are commonly operated by “doctors, computer scientists, and mathematicians” and are used to “obtain needed technology, send messages, cover up Al Qaeda-related travel, and raise money for their fighting” (Gaudin, 2001, pg. 48). By using these business fronts they have the ability to divert investigators and intelligence personnel away from the leader of the organization or rather the brains behind the operation.

It is suspected that Al Qaeda in particular has chosen steganography as a method of communication. Gaudin (2001, pg. 48) states that Al Qaeda still uses human messengers to transmit information so as to not leave a digital footprint. As mentioned earlier, a digital footprint is left, but some technology such as cellular phones and e-mails and can lead investigators straight to the origin of the message. Using a human messenger takes the digital footprint out of the equation, thus eliminating the evidence of communication.

Deficiencies in Data Supporting Steganography in Terrorist Communications

Although it is known that groups such as terrorist cells are using steganography it is still “not only difficult to find but also to decipher” (Sans Institute, 2001). The SANS Institute (2001) that many groups have found ways to make intercepting steganographic files difficult and "disseminating them very easy." This means that the ability to spread the file containing the hidden message is much easier yet harder for investigators to find.

In a paper written by Maura Conway of Dublin City University (2008) the author points out that much evidence shows knowledge of steganography being used, but no hard evidence showing the actual steganography. Conway sites an article in USA Today from February 2001, where Jack Kelley quotes, "special projects director for iDefense (a cyber-intelligence company) as saying 'the operational details and future targets, in many cases, are hidden in plain view on the Internet. Only the members of terrorist organizations, knowing the hidden signals, are able to extract the information'" (Conway, 2008).

In a follow-up article by Jack Kelley (2001) the author quotes then FBI director Louis Freeh stating, "Uncrackable encryption is allowing terrorists; Hamas, Hezbollah, Al Qaeda, and others, to communicate about their criminal intentions without fear of outside intrusion." As one can see it is not that the United States is in the dark as to what tools terrorist groups are using to communicate it is that the agencies investigating such activity do not know where the messages are being hidden nor do they have knowledge of the "hidden signals" (Kelley, 2001).

Audience

Knowing more about how terrorist groups use steganography allows the United States government to focus efforts on protecting national critical infrastructure. It will allow the agencies to develop policy to detect and counter terrorist communications. By using a risk management assessment much like the one created by Professor Randall K. Nichols, Dr. Daniel J. Ryan, and Dr. Julie J.C.H. Ryan (2000), the agencies could analyze the risks that come with terrorists using steganography**.**

LITERATURE REVIEW

Overview

"Cybercrime can often mutate into cyber-terrorism or occur simultaneously; cyber-terrorism by itself is a distinct entity" (O'Connor, 2011). New methods of communication between terrorist cells are surfacing. Studies show that cyber-terrorism is on the rise and those committing it are using steganography to communicate with one another (McCullagh, 2001). Dr. Tom O'Connor states, "The rates of cybercrime are skyrocketing and the annual take for the cyber-criminals are an estimated $100 billion" (2011). The purpose of this research is to examine the rise of steganography as a communication method between terrorist groups in order to carry out terrorist acts against the United States. In order to better understand why steganography is being used on must examine:

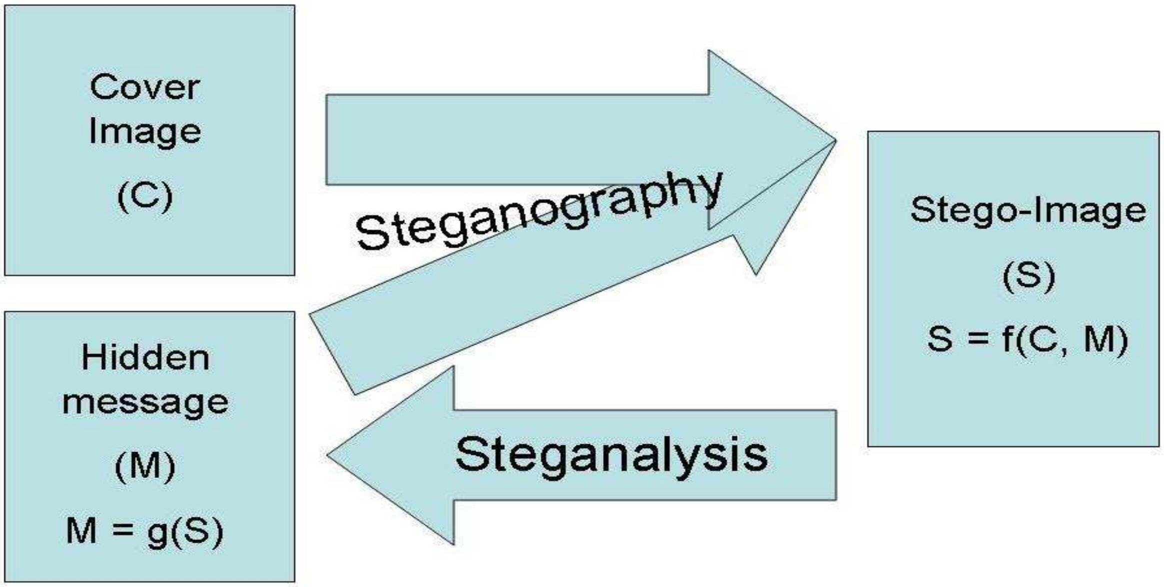
- What steganography tools are being used by terrorists to hide the communication?
- In what media do terrorists hide intelligence information and attack plans?
- What tools are available to find and "crack" steganographic messages?
- Does current DOD and Government security policy appropriately address steganography in terrorist communications? If not, what improvements are needed?
- What entities are employing steganography as a method of communication for the purpose of carrying out a terrorist attack?

Steganography is being used as a method of communication to commit cyber-terrorism acts against the United States (McCullagh, 2001). It has been used in some form for hundreds of years. Some date its use as far back as the days of Julius Caesar. James Judge discussed ways that the Greeks used steganography as far back as 480 BC. Judge states that, "a Greek by the name of Demaratus sent a message to the Spartans warning of a pending invasion by Xerxes. James Judge notes that the method used for communication at this time "was by scraping the wax off a pair of wooden folding tables, writing on the wood underneath (what Xerxes intended to do) and then covering the message over with the wax again" (Judge, 2001).

Steganography Primer

The art has drastically changed since ancient times. It is more advanced than ever. Steganography today is, "the art of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message" (Westphal, 2010). Simply stated, steganography is used to hide information in a host file. Figure 1 below illustrates the basic way in which steganography works (Codr, 2009).

Figure 1: Steganography Method



Source: *Unseen: An Overview of Steganography and Presentation of Associated Java*

Application C-Hide (Codr, 2009)

As shown by the figure above one chooses a "cover image" and a "hidden message" and then combines them. The result is a steganographic image that in plain view looks normal or unaltered (SANS, 2001). Steganography is commonly used to protect sensitive data that in the wrong hands could be damaging to either the individual or company said information belongs to (Radcliff, 2002). Deborah Radcliff writes for *Computer World*, "instead of protecting data the way encryption does, steganography hides the very existence of the data" (2002). Table 1 below shows some ways in which steganography is used to hide information of sensitive nature rather than as a method of criminal communication.

Table 1: Uses of Steganography

POSSIBLE USES OF STEGANOGRAPHY	**DRAWBACKS**
Used to combine explanatory information with an image (like doctor's notes accompanying an X-ray)	Could accidentally degrade or render an image misleading
Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission	Could counteract and be counterproductive with the original image
Peer-to-peer private communications	Doesn't hide the fact that an e-mail was sent, negating the purpose of secret communications
Posting secret communications on the Web to avoid transmission	Someone else with a steganography detection and cracking tool could expose the message
Copyright protection	A form of this already exists, called digital watermarking, but requires use of separate hardware

	tools because steganographic software can't use separate hardware tools. Steganographic software also can't protect the watermark.
Maintaining anonymity	Easier to open free Web-based e-mail or use cloaked e-mail
Hiding data on the network in case of a breach	Better to understand and effectively use standardized encryption

Source*: Reprinted from "Quick Study: Steganography: Hidden Data (Radcliff, 2009)*

As evident by the Table 1 above, steganography has long been intended for the protection of information. This was not an art intended for use in terrorist acts, but as the world evolves so do the terrorist networks aiming to attack the United States. James Judge (2001) states that, "after the events of September 11, 2001, there was an immediate concern voiced regarding the possible use of steganography by the al Qaeda network." Although it is appears to be common knowledge that terrorists are now using steganography as a method of communication the questions remains as to which countries pose a high threat to the United States, how they are using the technology, and where they are hiding the information (Judge, 2001).

China

When one thinks of a terrorist, one may think of someone affiliated with Iraq or Afghanistan, but what about China? In an article written by Robert Marquand and Ben Arnoldy for *The Christian Science Monitor* the author's state, "today, of an estimated 120 countries working on cyber warfare, China, seeking great power status, has emerged as a leader". China is not using cyber-attacks for religious beliefs, but rather for "political and military goals"

(Marquand and Arnoldy, 2007). Robert Marquand and Ben Arnoldy quote James Mulvenon, a Chinese Military expert and director of the Center for Intelligence and Research, stating, "Whether it is a battlefield preparation or hacking networks connected to the German chancellor, they are the first state actor to jump feet first into 21st century cyber warfare technology" (Marquand and Arnoldy, 2007).

Based on the previous statement one has to wonder who exactly is performing the attacks for China? According to Professor Randall K. Nichols, there are over 150,000 people that have been or are currently being trained in the craft of hacking on behalf of the Chinese government (Nichols, 2012). In 2010, the Internet Company Google announced that it had been attacked and those attacks were traced back to China. The *New York Times* reported in mid-February, 2010, that, "a series of online attacks on Google and dozens of other American corporations have been traced to computers at two educational institutions in China, including one with close ties to the Chinese military" (Markoff & Barboza, 2010). According to Joel Brenner the two schools in question were the, "Shanghai Jiao Tong University, a world-class computer programming school and Lanxiang Vocational School, which trains computer scientists for the People's Liberation" Army (Brenner, 2011). "For years, hackers with ties to the Chinese military have been eavesdropping on U.S. Chamber of Commerce Officials involved in Asia affairs, authorities say." According to a report by ABC News, Chinese hackers have accessed everything contained in the U.S. Chamber of Commerce computers, "including potentially, the entire U.S. trade policy playbook" (Thomas, 2011).

A group comprised of security professionals recently sat down and discussed hacking groups that pose the greatest threat to the U.S. The group tracked "an approximate tally of attackers targeting the intellectual property of U.S. and multinational companies: An even dozen, and all thought to be Chinese" (Lemos, 2011). With China appearing to be on the forefront of cyber-terrorism one has to ask how they are managing to infiltrate America's computers. Joel Brenner discusses the threat China poses to the U.S. in his new book *America the Vulnerable*, first asking, "how did the Chinese manage to remotely download up to twenty terabytes of information from the DOD, equal to 20 percent of all the data in the Library of Congress" (Brenner, 2011)? According to a spokesman for the Chinese Embassy, Geng Shuang, "cyber-attacks are prohibited by Chinese law and China itself is a victim of attacks (Gorman, 2011)." On the other hand, Joel Brenner states "economic espionage is intensifying." "The foreign intelligence services of China, Russia, Iran, and other countries are after our technology, and most of what they want is in the electronic-information systems of private companies; and the law and accounting firms that work for them" (Brenner, 2011).

Although, some members of the Chinese government may feel there is no "evidence or proof" that the attacks are originating in China, others state otherwise. According to Shane Harris, "computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and , in a few cases, gained access to U.S. critical infrastructure." Shane Harris states that "one prominent expert told *National Journal* he believes that China's People's Liberation Army played a role" in attacks against U.S. critical infrastructure" (Harris, 2008).

Not only is China hacking into U.S. government computers, "new evidence suggests China's hacking into drones using Adobe Reader and Internet Explorer." Sykipot, "a new computer virus having its way with the U.S drone fleet suggests the malware originated in

China" (Johnson, 2011). A report in *Information Week* "reports the virus appears to have been designed with the sole purpose of stealing UAV data using a 'zero-day' vulnerability in Adobe Reader" (Schwartz, 2011).

According to Robert Johnson, the Sykipot virus was "inserted into the military's network using an infected PDF file and specifically targeted to look for information on the Boeing X-45 unmanned combat air system and the Boeing X-37 orbital vehicle" (Johnson, 2011). In order for this to work, "the attackers used attachments that they feel recipients will find interesting." More notably, "all of the infections associated with a particular command and control (C&C) server for a Sykipot variant have been tied to phishing email that includes information about the two Boeing vehicles or systems" (Schwartz, 2011). Knowing who is performing these types of attacks is not enough however; it is in the interest of the protection of National Security to find out where they are hiding their malware and communications.

Hiding in Plain View

Steganography, as stated previously, is the art of hiding data such as a text document within a carrier file so it is not seen by unwanted eyes. When using steganography in cyber warfare one has to look at where the information is being hidden. Tom Kellen of the SANS Institute discusses how steganography is used to hide information in "plain view (Kellen, 2001)." Many United States officials and experts in the field have gone on record stating that terrorists, or rather cyber terrorists, are "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites" (Schneier, 2001).

The Internet contains a world full of photographic images that could be used as a host file. “Cyberspace has become a home for vice and evildoing” (O’Connor, 2011). According to Tom Kellen, “it has been suggested that terrorist groups posted carrier files on porno sites which may seem an ironic place to hide files but this would go along with the premise of hiding in plain view” (Kellen, 2001). Pornographic web sites are a common place to hide communications as the graphic files contained on these sites are usually very large and use a lot of color. “These would make ideal carrier files since the larger the carrier file, the larger the payload it can carry” (Kellen, 2001).

In 2004, Gary C. Kessler discussed the use of steganography as a tool for child pornography trafficking. He stated that one could put an item up for sale on eBay that is a legitimate item, put new photos of the item up that contain hidden information, and the receiver would know exactly how and when do retrieve the information. This is very similar to what is being done by terrorists, but instead of hiding pornographic images they are hiding covert communications (Schneier, 2001). Bruce Schneier discusses the link between terrorists and steganography by relating it to a well-known “insider,” Robert Hanssen. Bruce Schneier states, “using steganography to embed a message in a pornographic image and posting it to something like a Usenet newsgroup is the cyberspace equivalent of a drop dead” much like Robert Hanssen using, “signals to communicate with the Russian handlers he was dealing with” only on a digital level (Schneier, 2001).

In 2004, Professor Randall K. Nichols discussed the use of steganography by terrorists and brought to light the hiding of communications within porn sites as well as spam e-mails. Professor Nichols pointed out that although a group of researchers from the University of Michigan analyzed over 2 million possible carrier files with “good statistical techniques” they did not look at porn or spam. How terrorists are using e-mail as a method of communication is still being investigated. According to Joel Brenner, the Chinese have used a method called "phishing" to infiltrate the various government networks. When it was discovered that China hacked the Internet Company Google, "the caper was enabled by an expertly targeted phishing expedition." The attackers "generated fake e-mails that seemed to come from another executive whom the target knew, so the target clicked on it, clicked again on a hot link or an attachment and the attackers were in" (Brenner, 2011).

Aside from attaching links, SPAM is used as a host for steganography messages. Much like the phishing used to transport malware; cyber-terrorism groups use SPAM to exchange communications between one another. According to Tomer Ben-Ari, cyber media such as e-mail, including spam is used as a "mass-communication tool to plan and coordinate terror attacks" (Ben-Ari, 2006). Spam can also be used as a method of theft or denial of service. If the e-mailer sends a large amount of Spam mail to one server it can cause the entire system to crash or at the least be denied service (O'Connor, 2010).

Table 2: Media Used by Terrorists

Type of Cyber-Media	**How it is used by terrorists**
E-mail	To attach a file containing malware for a target to open unknowingly

SPAM	To attach a steganographic image containing a document with communications that is only accessible by the receiver holding the "private key"
Website	To hide communications within an image on the website accessible by the receiver only
Mobile Device	To hide communications within a small image, sound file, or voice recording

Source: *Adapted from: Terror Spam and Phishing* (Ben-Ari, 2006)

Jack Kelley for *USA Today* quotes former U.S. Attorney General Janet Reno stating, "in the future we may tap a conversation in which the terrorist discusses the location of a bomb soon to go off, but we will be unable to prevent the terrorist act when we cannot understand the conversation" (2001). Although, Janet Reno is discussing the possibility of terrorists disguising their voices in the previous quote, Kelley points out that disguising e-mails is currently being used as well. Just as Professor Nichols discussed, spam e-mail is yet another way that terrorists can disguise their communications between one another (2004). Jack Kelley discusses covert communications stating, "They are hidden using free encryption Internet programs set up by privacy advocacy groups. The programs scramble the messages or pictures into existing images. The images can only be unlocked using a "private key," or code, selected by the recipient (Kelley, 2001).

Steganography Tools

In order to hide communications or sensitive information cyber-terrorists are using various media types combined with steganography programs that are both available for purchase or open-source tools (Kessler, 2001). According to Chet Hosmer, Chief Scientist, and Senior Vice President of Cyber Security at WetStone Technologies, one should understand the difference between a large and small communication message and that of a time-sensitive matter. “The type of host file used may vary depending on the type of message being sent” (Hosmer, 2012).

A small message may consist of simple instructions being sent from one member of an organization to another. In order to hide a small file one has the ability to use a smaller host file. According to Gary Kessler, audio and image files are considered the most common type of digital carrier files to date. He states that these files are more commonly used “because of the plethora of possible carrier files already in existence (Kessler, 2011).” An image file, such as a photograph obtained from Internet, can be used as a carrier file to hide a simple word document within it.

A large message, much like an attack plan with pictures or maps, may be hidden in a much larger host or carrier file. In an article written by Brad Astrowsky for the Anti-Child Pornography organization, the author states “there are over 4,000 sites dedicated to steganography making it easier to hide information.” That being said, images on a child pornography site, as mentioned earlier, are image files that are large enough to conceal a large message being sent” (Astrowsky, nd).

Multimedia carrier files are also being employed to hide communications. Using multimedia occurs when one uses multiple platforms to hide and send the covert message. This is often done through the use of cellular or mobile device and they are capable of transmitting images, voice recordings, and videos within a seemingly innocent text message. Mobile devices have been found to be a discreet, easy to use tool for both hacking and covert communications. Joel Brenner points out that the "computing capacity greater than governments could muster during the cold war now resides on mobile devices" (Brenner, 2011). By using mobile devices the terrorist becomes more covert and mobile themselves rather than having to remain in one location for a long period of time.

According to Chet Hosmer, the Internet is an ideal place to hide covert communications. It is the most common way to hide communications "in plain sight." Chet Hosmer stated that one of the biggest reasons this method is used to hide communications is that the "adversary creates a haystack and we have to find the needle" (Hosmer, 2012). There are millions of people accessing billions of websites every day and to track the one person who leaves a covert message out in the open on the web would be extremely difficult.

The other major type of communication one must look at is that of a time-sensitive file. eBay, as discussed earlier, is a prime location for a hidden message. According to the Center for Information Technology Integration, eBay is used because it is "a very organized web structure that facilitates downloading images pointed to by auctions" (CITI, 2002). Cyber-terrorists can simply load an image that appears to be for sale in an auction and hide information within the image loaded. This works well for time sensitive information as the terrorists can organize a time to load the image and a window of time for it to be retrieved by the receiver (Provos & Honeyman, nd).

Table 3: Media Used for Covert Communications

Type of Communication	Media Used	Why it is used
Small Message	Small image, audio, or video files	To send small communications or images
Large Message	Large image, audio, or video file (i.e. movies, audio books, or pornographic images	To send large covert communications such as maps, attack plans, or large private messages
Time Sensitive Message	Large video or image file such as movies, pornographic images, or auction items	To hide large communications to be uploaded at a specific time pre-arranged with the receiver

Source: *Adapted from: Steganography: Hiding Data within Data* (Kessler, 2001)

Knowing how the images are being hidden is a start but one must also know what tools are being used in conjunction with the carrier files. After all, it takes a steganography program to create a carrier file. Chet Hosmer has created or helped create many steganography tools throughout his career. WetStone Technologies is known for its steganography detection tools such as Stego Suite, but what about the tools that are used to hide the information (WetStone Technologies, 2012). There are hundreds of tools available including some that were created for the purpose of protecting sensitive information, not for use by cyber-terrorists. Table 4 below shows a sample of some tools available and their features.

Table 4: Sample of Steganography Tools

Tool	Cost	Features
Steganos Safe 2012	\$39.95 - \$79.95	• Highly secure encryption • Vaults up to 1 Terabyte • Portable Safe • Invisible • Steganos Shredder • Quick and Easy
Dound's Steganographer	Free	• Private • Easy • Unique • Encode and decode
Xiao Steganography	Free	• Five encryption algorithms • Four hashing algorithms • Does not alter images • Password protected
Spammimic	Free	• Encode • Decode • Create spam messages • Hide all sizes of files
Steghide	Free	• Compression of encrypted data • Compression of embedded data • JPEG, BMP, WAV, and AUP files
QuickStego	Free	• Hide data within an image • JPEG and BMP
QuickCrypto	£24.99 (≈\$39.00)	• Conceals data in folders, images, and sounds

Source: *Adapted from: CNET Downloads* (CNET, 2012)

Steganos Safe is a program created by a German software company, GmbH, which is capable of hiding information in a secure, vault-like method. According to the creators, the program is ideal for use by those who want to protect information, images, and communications (GmbH, 2012).

Dound's Steganography is freeware available on the Internet to anyone. It allows the user to create a carrier file that may be sent in an e-mail or even uploaded on the web. This tool requires a password that is created by the sender and then used by the receiver to obtain the communication (Dound's, n.d.). Xiao Steganography is another tool capable of hiding information. It allows the user to hide data within a carrier file of their choice and protect with one of five encryption methods and four hashing algorithms (CNET, 2012).

As previously mentioned, cyber-terrorists have the ability to hide information within an e-mail or spam message. One tool that is capable of converting a communication into a spam message is Spammimic. Spammimic is a tool that can both encode and decode a communication into a spam message. It simply converts the message to a spam message allowing the sender to pass the message along without detection (Spammimic, 2010).

All of the aforementioned tools have the capabilities of hiding various sizes of communications in a "plethora" of carrier files. They can all hide information in plain site or in a hidden location depending on the choices of the creator. According to Josh Hally, even though steganographic messages are hard to detect and often not found, the risk still remains. The method is being used and the number of people employing the method is increasing (Hally, 2002).

Risk Management

Managing the risk of an attack is crucial to the protection of the U.S. intelligence information. The FBI Counterintelligence National Strategy, in discussing the protection of U.S.

Secrets, states “we see it, and work hard to counter it, all the time” (FBI, 2011). When discussing the protection of the secrets of the U.S. intelligence community the FBI stated that “using intelligence to focus our investigative efforts and collaborating without government partners to reduce the risk of espionage and insider threats” (FBI, 2011). Partnerships are a large area of focus for the FBI when dealing with the possibility of cyberterrorism.

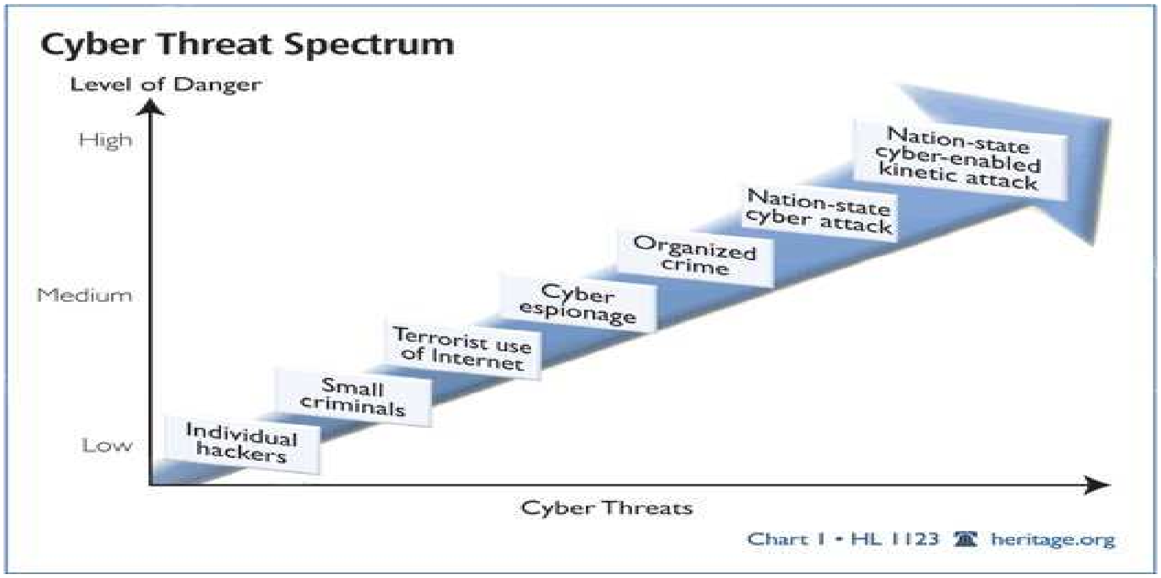
In an article titled “*A Blueprint for Protecting U.S. Secrets*” written by the FBI partnerships are a main strategy for the protection of U.S. intelligence. The article discusses three areas of focus:

- “the sharing of expertise and resources of the FBI, the U.S. intelligence community, other U.S. government agencies, and global partners to combat foreign intelligence activities
- Coordination of U.S. intelligence community efforts to combat insider threats among its own ranks; and
- Partnerships with businesses and colleges and universities to strengthen information sharing and counterintelligence awareness” (FBI, 2011).

Collaboration with other agencies is a key focus for the protection of information that pertains to the United States national security. Being able to identify the risks facing the United States and how to manage those risks is imperative to the protection of U.S. Intelligence. In a testimony by Brett Hovington, Chief, Community Relations Unit, Office of Public Affairs, FBI Mr. Hovington discusses the, “FBI’s community outreach and engagement efforts to build trust and open constructive dialogue with American Arab, Muslim, Sikh, Somali, Asian, and South Asian communities” (Hovington, 2010). Brett Hovington states that the key to, “stopping future generations from fighting against our country instead of for it, we must commit to increasing our field-based scientific research on the violent radicalization of youth" (Hovington, 2010). By openly communicating with other countries, Brett Hovington states that in order to manage risk, open partnerships, and communication must be present.

Collaboration aside, risk assessment ultimately comes down to the level of threat one faces. Dr. Tom O'Connor discussed a threat assessment in a recent lecture the fact that the more appealing an attack scenario seems, the more likely the intent to harm will rise (2011). Figure 2 below shows the cyber threat spectrum that Dr. O'Connor discussed starting with a low risk threat or level of danger and ending with a high risk threat or level of danger. As one can see the level of threat can vary based on the number of individuals involved. An attack could involve an individual hacker or an entire "nation-state." However, no matter how small or large the threat any of them can cause irreversible damage to the victim. Whether it is a "botnet attack, an attack on critical infrastructure, or a large scale attack on a government agency; "the permutations are as endless as one's imagination" (O'Connor, 2011).

Figure 2: Cyber-Threat Spectrum



Source: *Cyber Threat Spectrum* (O'Connor, 2011)

As one can see, the lowest threat is that of an individual hacker. As the crime increases, for example, espionage, organized crime, or cyber-attacks, the level of threat increases. According to Dr. O'Connor, understanding when the threat becomes greater is key to determining the level of risk involved (O'Connor, 2011).

Along with collaboration and risk assessment, proper policies are imperative in the defense against cyber-attacks. Acceptable Use policies can prevent an innocent person from opening something that contains a covert message. "Defining a clear policy is the first step to security. Acceptable Use Policies (AUP), also known as Internet Access Policies (IAPs), stress organizational expectations of Internet usage. By setting guidelines, companies emphasize that Internet access at work is a privilege, rather than a presumptive right. According to M86 Security, an acceptable use policy is a set of "norms of protocols, regulation, and 'digital behavior' rules that limit the security risks for any organization" (M86, 2012).

According to Chet Hosmer, along with proper policies any organization needs to ensure that their employees understand the policy they have to follow. This is done by more than having each employee read the policy and sign a form. Constant training is necessary to ensure that everyone fully understands the policy requirements and the consequences that go with ignoring them (Chet Hosmer, 2012).

Recap

Understanding how and why cyber-terrorists are turning to steganography as a method of communication is vital to assessing the risk they impose. The purpose of this paper is to examine the how and why behind the use of steganography in cybercrime such as cyber-espionage and cyber-terrorism by answering the following questions:

- What steganography tools are being used by terrorists to hide the communication?
- In what media do terrorists hide intelligence information and attack plans?
- What tools are available to find and "crack" steganographic messages?
- Does current DOD and Government security policy appropriately address steganography in terrorist communications? If not, what improvements are needed?
- What entities are employing steganography as a method of communication for the purpose of carrying out a terrorist attack?

According to Professor Randall K. Nichols and Chet Hosmer, a variety of tools are being used by cyber-terrorists. Whether the tools are for purchase or open-source they are being employed by terrorist groups (Chet Hosmer, 2012). The tools being used afford the terrorists the ability to spread their communications on multiple platforms or medias. Gary Kessler points out that many terrorist groups use audio or image files of various sizes as host files for a covert communication. He states that using a host file such as the aforementioned the sender can conceal the message within an everyday e-mail therefore making it appear as a normal message (Kessler, 2001). Not all tools are being used by cyber-terrorists for covert communications. There are hundreds of tools available that are capable of detecting steganography. WetStone Technologies is on the forefront of creating such tools. Programs like Stego Suite have the capability analyzing a specific media file for many markers that are more commonly found in steganographic messages (WetStone Technologies, 2012).

Aside from regular e-mail messages communications are being hidden in large file types such as a large picture, typically one from a pornographic website and placed on the Internet. According to Chet Hosmer, the reason the Internet is widely used is because there are so many people accessing certain sites that it makes it more difficult for the sender and for that matter the receiver to be traced (Chet Hosmer, 2012). Spam e-mail is commonly used by terrorists as well as regular e-mail because there are many tools that allow the sender to conceal their identity as well as a covert message within it. Spammimic does just that, it allows a user to hide or convert a message in order to conceal it from unwanted eyes (Spammimic, 2010).

Policies, especially Acceptable Use policies, are vital in the protection of any organization's information. M86 Security advises that a policy should cover all basis and if necessary be "industry specific" where necessary. With the proper acceptable use policy a company keeps things in "order" and ensures that chaos associated with the Internet, such as cyber-attacks stays away (M86, 2012).

With the rise of steganography as a method of communication the question as to who is leading the pack on cyber-attacks and cyber-terrorism comes up. The answer, according to many is China. It has been proven on multiple occasions that China has been behind many attacks against the U.S. (Markoff & Barboza, 2010). Professor Randall K. Nichols discussed recently that China has the ability to commit such attacks because they are "state sponsored' and they are constantly training thousands of individuals to become better "hackers" for the sole purpose of attacking the U.S. (Nichols, 2012).

With all of the research that is currently in books, written in white papers, and on the Internet all signs point towards China as the greatest threat to the U.S. That being said understanding what can be done to protect an organization's information against such threats is imperative. Knowing which tools to use for analysis and what types of policies to implement can only help an organization much like that of the DOD. By continuing to do research on how and why countries such as China are using new methods such as steganography as a communication tool for cyber-attacks the U.S. will only be able to improve their protection of information (Gray, nd).

DISCUSSION OF FINDINGS

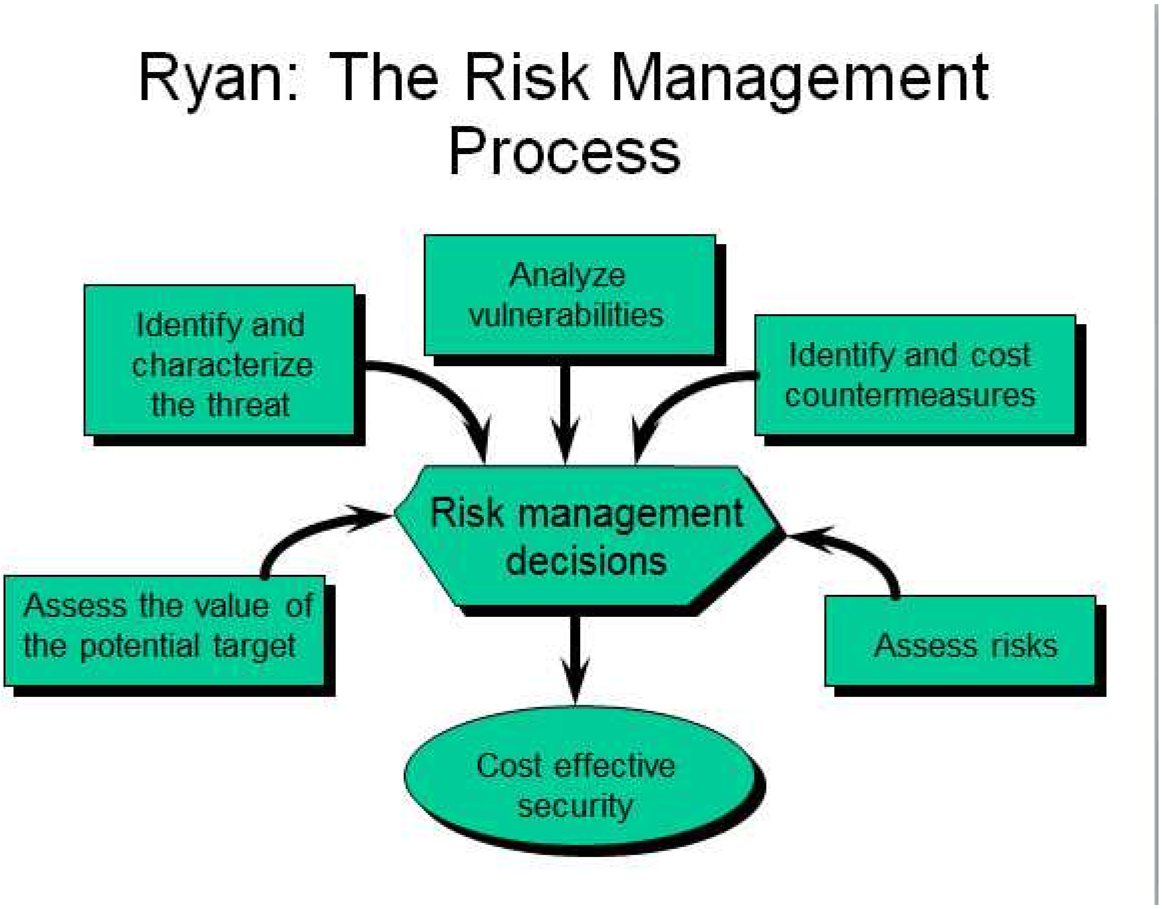
Research Synopsis

Cyber-terrorists are finding new ways to communicate with each through covert channels. “Cyber-terrorism involves a specific national security target but can easily escalate into a full-scale infrastructure attack on a whole society, depriving inhabitants of electrical power, dam protection from floods, or use of emergency services” (O’Connor, 2011). In recent years, the use of steganography is on the rise as one method of communication being used by hiding a message within a host file and sending it through e-mail or posting it on the Internet. Steganography allows the user to conceal a message for a specific receiver in a manner undetectable to the naked eye (McCullagh, 2001).

The researcher focused on select areas to better understand steganography as a method of communication and who is employing it for the purpose of committing cyber-terrorist attacks against the United States. “The potential threat posed by cyber-terrorism has provoked considerable alarm. Numerous security experts, politicians, and others have publicized the danger of cyber-terrorists hacking into government computers, including the military” (USIP, 2011). In order to better interpret the evidence pointing to whom, what, and why one needs to understand; who is on the forefront of the cyber-terrorism movement, what methods of communications are being used, and how and why they are using said methods.

While knowing who is a threat and what methods they are using is imperative any organization dealing with cyber-terrorism must analyze the risk that comes with any threat. Professor Randall K. Nichols and two of his colleagues, Dr. Daniel J. Ryan and Dr. Julie J.C.H. Ryan, explained risk management in detail in their book *Digital Assets Against Hackers,* *Crackers, Spies, and Thieves* in depth. Risk management should be looked at from multiple angles. Figure 3 below shows that one must "identify and characterize the threat, analyze vulnerabilities, identify and cost countermeasures, assess risks, assess value of a potential target, and cost effective security" (Nichols, Ryan, & Ryan, 2009).

Figure 3: Risk Management Process



Ryan: The Risk Management Process

Identify and characterize the threat
Analyze vulnerabilities
Identify and cost countermeasures
Risk management decisions
Assess the value of the potential target
Assess risks
Cost effective security

Source: Cybersecurity: A Future in Crisis? NYSETA Plenary (Nichols, 2009)

By analyzing all angles of a risk management decision one can visualize the top threats that may face an organization, especially an agency such as the DOD, FBI, or NSA, all of which deal with information that may be essential to the U.S. national security.

Greatest Threat

“At least a dozen countries are developing programs to attack other nation’s information and computer systems, many of which are hostile to the United States” (Pope, 2008). According to a study done by LCDR Lonnie Pope of the U.S. Navy the People’s Liberation Daily in China stated that “all a foe to the U.S. had to do was ‘mess up the computer systems of its banks by high tech means. This would disrupt and destroy the U.S. economy” (Pope, 2008). In an article for *The Washington Times* Eli Lake discussed a statement by the Director of National Intelligence, James Clapper saying “China is considered the most significant threat among nation states, with Russia posing the second-greatest threat” (Lake, 2011).

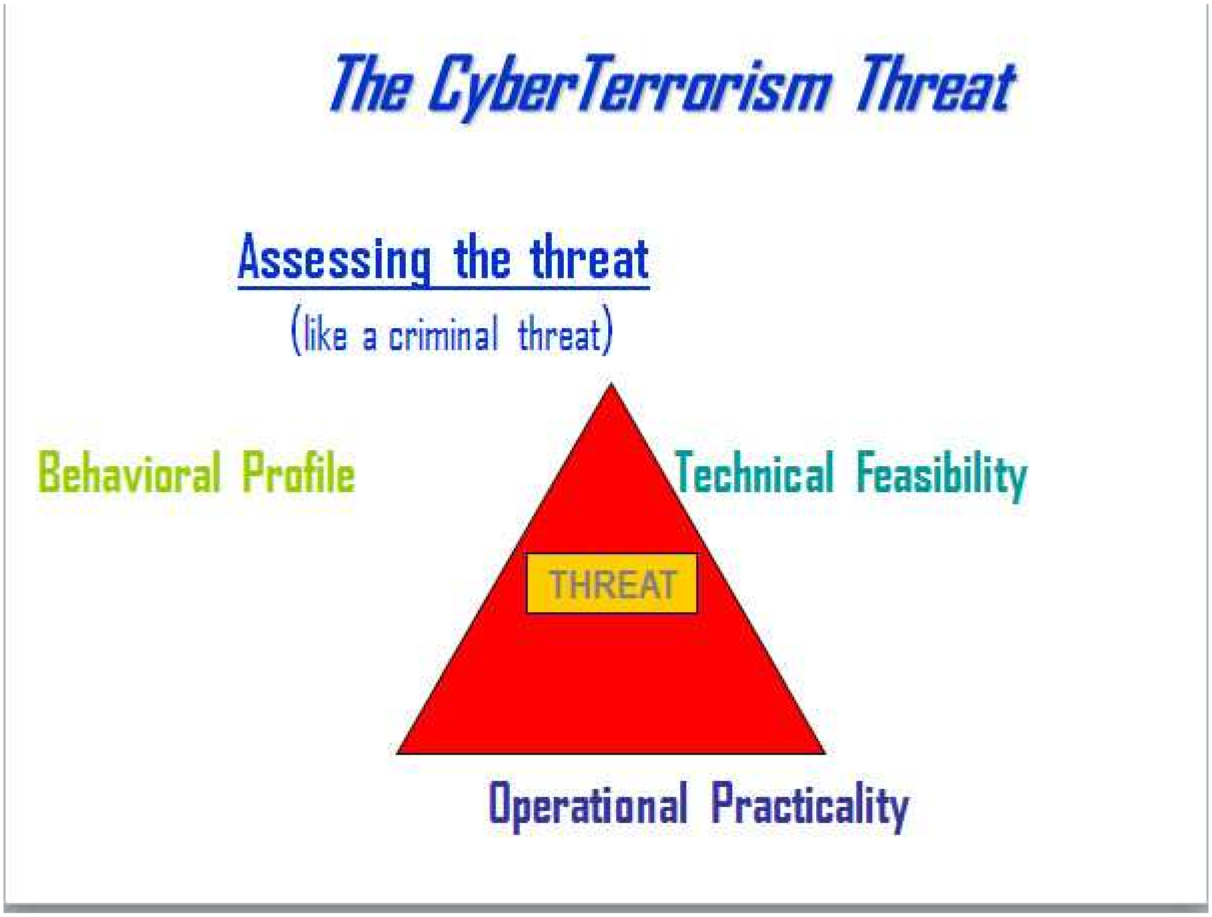
When analyzing steganography as a tool for communication one has to consider which countries are developing the threat technology. According to Chet Hosmer, those countries or areas currently at the forefront of developing such technology are Eastern Europe, China, and the U.S. The technology is being developed based mainly on the demand for newer tools and ways to carry out covert communications (Hosmer, 2012). One has to then ask who is buying and using the threat technology being invented. Currently; Iran, Iraq, Afghanistan, and North Korea are among the greatest threats to the U.S. that are buying and employing the use of threat technology. Countries such as those mentioned are using the newly developed technology based on their need for more covert methods of communications. In order to keep countries such as the U.S. at bay, new methods are continuously being developed and employed (Hosmer, 2012).

“According to successive Pentagon reports to Congress, China is currently building its strategic nuclear forces and has spurned offers from the administration to begin talks on cyber-weapons” (Lake, 2011). In order to assess how great a threat a country such as China is to the

U.S. one has to first understand the "Cyber-terrorism Threat." Professor Randall K. Nichols discussed such a threat triad in a 2009 lecture that can be seen in Figure 4 below. The cyber-terrorism threat takes the behavioral profile, technical feasibility, and operational practicality as the three keys to assessing a cyber-terrorism threat (Nichols, 2009).

The first part of the triad is behavioral profile which deals with the behavior of the cyber-terrorism suspect. In the instance of China, one would have to understand the common behavioral patterns of the Chinese government in past cyber-attacks.

Figure 4: Cyber-Terrorism Threat



Source: Cybersecurity: A Future in Crisis? NYSETA Plenary (Nichols, 2009)

Aside from the behavior of a threat one has to analyze the feasibility of an attack occurring. According to Teppo Kivento, technical feasibility is when a "product or service can operate in its desired manner." In other words, can the tool being used feasibly attack the victim system, for example a DOD computer system (Kivento, 2006)?

Operational practicality is the third part of the cyber-terrorism threat discussed. By operational practicality one must understand whether or not the operation in question is functional. If one used the triad above to analyze China they would have to know common behavioral patterns of China, whether or not they possess the technology to carry out the threat or attack and will that technology will operate correctly, and finally is the threat a functional one (Nichols, 2009)?

Covert Communications

Covert channels of communication are constantly being used by terrorist groups. According to the U.S. Department of Defense a covert channel is "any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy." "Covert storage channels include all vehicles that would allow the direct or indirect writing of a storage location by one process and the direct or indirect reading of it by another. Covert timing channels include all vehicles that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information" (Owens, 2002).

Steganography "is far from a new science" and is now being used by terrorist cells as a method of communication through covert channels. A prime example of this is the ability of a user to alter an audio file so it may hide a communication between terrorists. If one takes an audio file and "overwrites the lowest byte of data" it will not alter the quality of the media and therefore will be harder to detect with a steganography tool (Scorbett, 2004).

According to Professor Randall K. Nichols, steganography combined with coded SPAM e-mail is one way that a country like China could attack or pose a threat to the U.S. By coding a SPAM message with a tool such as Spammimic combined with a cryptography tool like CryptPix or Cryptflix the terrorist as the capability of not only hiding the covert message, but also hiding it in a seemingly innocent e-mail message (Nichols, 2004). The problem with this type of communication is that human error is likely. When one opens an e-mail and inadvertently "clicks" on a link or photo which in turn opens a covert message that can cause damage to a system. Human error is a major reason the U.S. is attacked from within its own agencies which is why Professor Randall Nichols recommended that people simply delete a suspicious e-mail or SPAM message immediately (Nichols, 2004). He also recommended a complete cleaning of the computer slack space every day the Internet is accessed (Nichols, 2012).

SPAM, images within e-mails, and pornography sites are the main places that cyber-terrorists will hide *stego* communications. China, however, is not the only country hiding information in plain sight. According to Professor Randall K. Nichols various other countries are now turning to using covert communications like steganography as a method of planning and communicating attacks against others such as the U.S. Table 5 below shows which countries pose a risk to the U.S. based on their use of steganography and even cryptography (Nichols, 2004).

Table 5: Countries Employing Steganography or Cryptography

China	Brazil	United Kingdom	Taiwan
Germany	Japan	Italy	Malaysia
Australia	Poland	Turkey	Mexico
Argentina	Saudi Arabia	Thailand	Pakistan
Czech Republic	Moldavia	Yemen	Morocco
Philippines	Israel	South Korea	North Korea

Source: Adapted from: Trust Me It's Encrypted (Nichols, 2004)

As can be seen by the table above, the "global terror network" is much greater than many believe it to be. According to Professor Randall K. Nichols even the use of an "extra paragraph is perfect for Steg and has at least 500 characters; it creates steganography within a null" (Nichols, 2004). Knowing that more than just China is a risk to the national security of the U.S. one has to understand how to analyze said risk. The Ryan-Nichols Equation is one that analyzes the risk of something based on threat, vulnerabilities, impact, and counter measures. Figure 5 below shows the Ryan-Nichols equation used to analyze the risk of an event (Nichols, 2004).

Figure 5: Ryan-Nichols Equation

Ryan-Nichols Risk Equation

$$\textit{Risk} = \frac{\textit{Threats x Vulnerabilities x Impact}}{\textit{Countermeasures}}$$

Source: Adapted from: Trust Me It's Encrypted (Nichols, 2004)

The equation looks at the threat as a whole and then takes four other factors into consideration. To begin one has to create the scale to weigh the risk. In the instance of cyber-terrorism, if one were to use a scale of 1-5 the analyst would add all of the numbers (1+2+3+4+15) and use that answer as the overall weight to divide the equation by (Nichols, 2012). Table 6 shows how one would do a risk analysis on just a few countries that may pose a risk to the U.S. By using a scale of one through five the researcher will show the possible risk that China, Russia, Al Qaeda, and a category of "other" pose toward the U.S.

Table 6: Ryan-Nichols Equation at Work

Country or Terrorist Group	Threats	Vulnerabilities	Impact	Counter-measures	Risk
China	**Medium High** Cyber terror attack carried with the use of steganography	**Medium** • Human error • Policy and procedures to lessen impact	**Medium High** • Loss of sensitive data • Loss of critical infrastructure functionality	**Medium** • High computer security • Trainings of personnel • Acceptable use policies	**Medium** .53 or 53%
Al Qaeda	**Medium High** Cyber terror attack carried with the use of steganography	**Medium** • Insider threat • Human error	**Medium** • loss of innocent lives • loss of critical infrastructure	**Medium** • Acceptable use policies limiting insider threat • High computer security	**Medium** .40 or 40%
Russia	**Medium** Cyber terror attack carried with the use of steganography	**Medium** • Human error • Policies not in place	**Medium** • Loss of critical information • Loss of critical infrastructure	**Medium** • Personnel trainings • Computer security tools	**Low** .04 or 4%
Others	**Medium Low** Cyber terror attack carried with the use of	**Medium Low** • Human error • Insider threat	**Medium** • Loss of data	**Medium** • Computer security tools • Computer security training	**Low** .03 or 3%

	steganography				

Source: Adapted from: Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves (Nichols, Ryan, & Ryan, 2000)

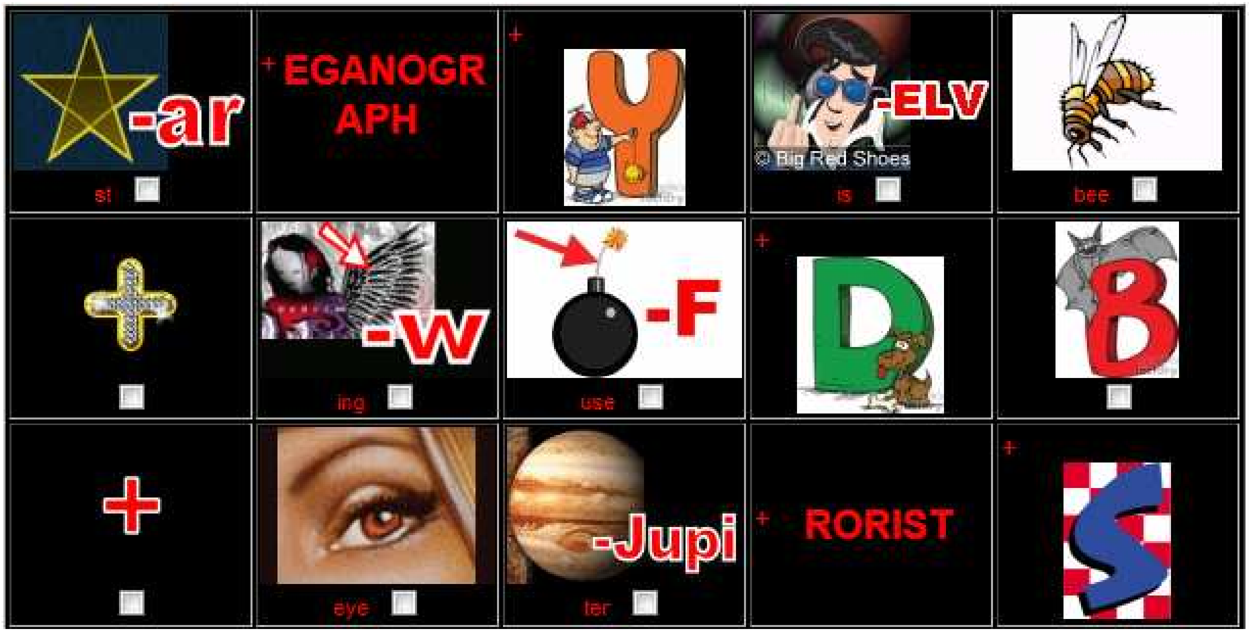
As seen in the table above, by assigning a level for each component of the equation the risk analysis shows that both China and Al Qaeda pose the greatest risk to the U.S. at this time and Russia, although less of a risk, poses a low level threat to the U.S.

Tools Assessment

Steganography tools are not only being used to detect steganography as one can see by the rise in the use of steganography by cyber-terrorists. Companies like WetStone Technologies create steganography tools for the purpose of detecting hidden messages, not committing crimes. Stego Suite, for example, has the ability to detect over 500 different steganography hiding programs, analyze art and audio images, and crack and extract “payloads” from a carrier file (WetStone, 2012).

The cyber-terrorists, however, use hundreds or tools such as CryptoPix or CryptoFlix are being used to disguise messages in images, audio files, and websites; especially pornographic sites. CryptoPix allows the user to simply type their messages into the text box and the program converts it to a set of images that are equivalent to the original text as show in Figure 6 below.

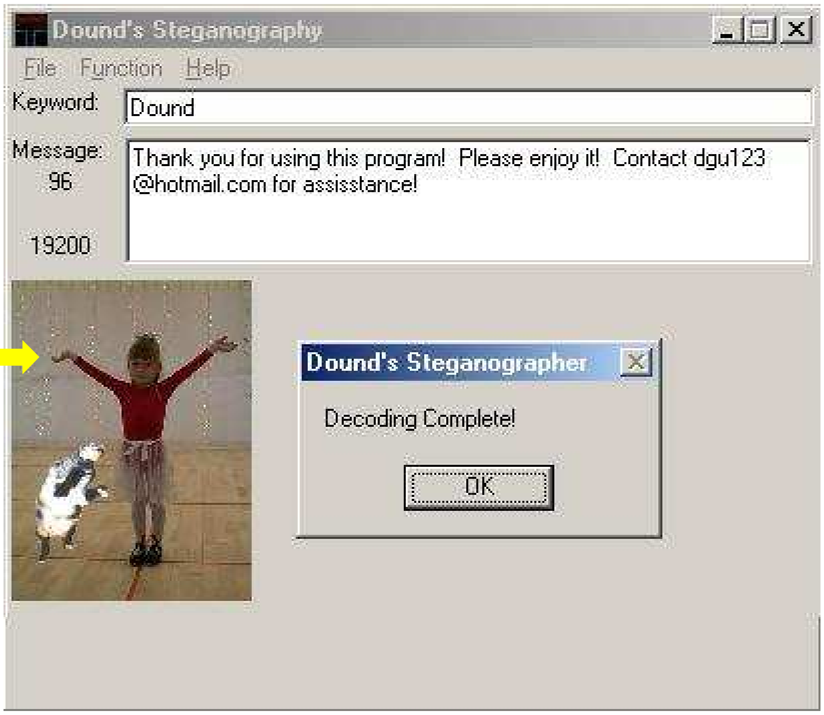
Figure 6: CryptoPix Example



Source: Reproduced from: CryptoPix Message Creator (CryptoPix, 2008)

Other programs, much like Dound's Steganography, use an image or audio file as a carrier or host file and hid the message within using a keyword or password. Figure 7 below shows an example of how Dound's Steganography works.

Figure 7: Dound's Steganography



Keyword: Dound

Message: 96

19200

Thank you for using this program! Please enjoy it! Contact dgu123 @hotmail.com for assisstance!

Dound's Steganographer

Decoding Complete!

Host file

Source: Reproduced from: Dound's Steganography (Dound's, nd)

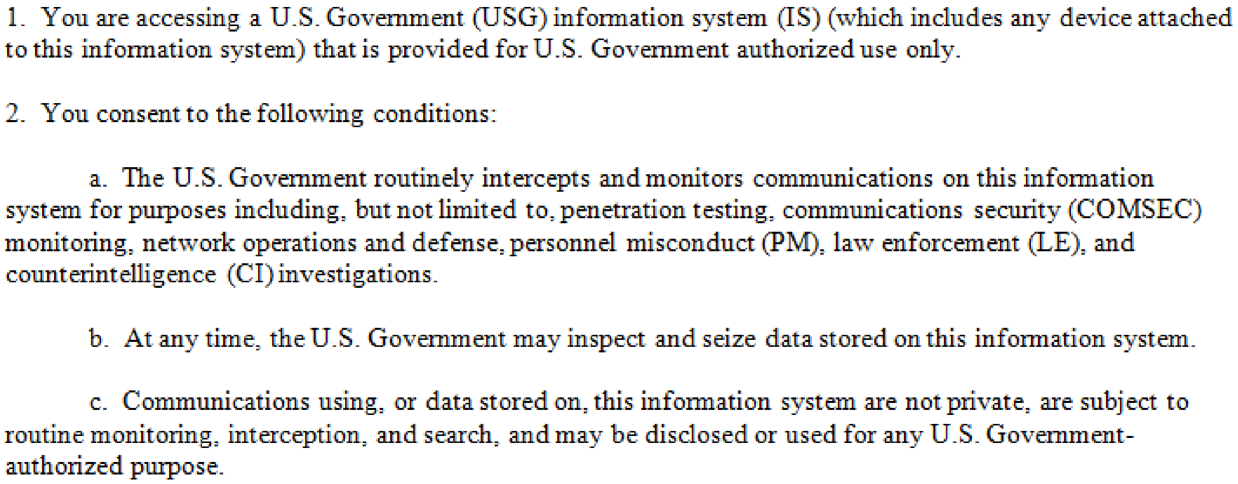
In a study done at the University of Michigan, Peter Honeyman and students analyzed millions of e-mail messages for steganographic messages finding nothing. This does not mean these covert messages do not exist. Professor Randall K. Nichols analyzed the same data and was able to see that not only was there steganographic messages, but they were contained in attachments, SPAM messages, and pornographic websites (2001).

Since steganography is currently rising as a method of communication between terror cells one must remain aware that with the rise of demand for a product comes product creation and upgrading. Steganography tools are constantly evolving and although companies like WetStone Technologies and AccessData are continuing to create tools that detect covert communications and their programs. Those that create the tools to hide the information are creating or upgrading their own programs or cyber-war weapons just as frequently if not more so (Judge, 2001).

Policy Assessment

As advantageous as it is to have state of the art steganography detecting programs, simple policies can help mitigate cyber-attacks just as well. Most companies have an acceptable use policy for all employees accessing any computers. The DOD has an acceptable use policy that limits the use of their computers and notifies the employee signing the policy agreement as to their rights and privileges as they pertain to the company. Figure 8 below contains a small portion of the acceptable use policy signed by all affiliated with the DOD.

Figure 8: Acceptable Use Policy



1. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

2. You consent to the following conditions:

a. The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

b. At any time, the U.S. Government may inspect and seize data stored on this information system.

c. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

Source: Adapted from: AUP (DoD, 2012)

Most AUPs explain, in detail, what the rights of the company or agency are to seize a computer at any time or anything contained on the computer. Even if someone signs an AUP it does not mean they understand what they are trying to find. As stated earlier in this paper, human error is a major vulnerability of cyber-terrorism. Someone could simply click on the wrong item exposing their agency to an attack (M86, 2012).

According to Chet Hosmer of WetStone Technologies, although policies are great and work for the most part, they create a “false sense of safety.” People tend to think that just because they read the policy does not necessarily mean they understand it. Chet Hosmer stated that through ongoing training helping employees better understand the policies an agency helps to secure their data more, if not a great deal , at least a bit better (Hosmer, 2012).

With any risk come threats as well as vulnerabilities. What one does to counter-measure the impact can weigh heavily on any analysts mind? It can become a matter of national security if a risk is not dealt with properly. That being said the researcher has some recommendations as to what an agency such as the DOD, FBI, or CIA may want to incorporate, implement, or change in order to better protect their information and analyze the risk of a cyber-threat (based on the cyber-terrorist country).

RECOMMENDATIONS AND CONCLUSIONS

CONCLUSIONS

The rise in both cyber-terrorism and steganography as a communication tool raises many questions as to how the acts are being carried out and the threat they may pose to the United States (McCullagh, 2001). *The purpose of this research was to examine the rise of steganography as a communication method between terrorist groups in order to carry out terrorist acts against the United States.* The researcher analyzed:

- What steganography tools are being used by terrorists to hide communications?
- In what media do terrorists hide intelligence information and attack plans?
- What tools are available to find and "crack" steganographic messages?
- Does current DOD and Government security policy appropriately address steganography in terrorist communication? If not, what improvements should be made?

The researcher analyzed which countries pose the greatest threat to the U.S. and how they may be using methods such as steganography as a covert communication tool. China is considered to be the greatest threat to the U.S. with Russia following behind at a close second (Marquand and Arnoldy, 2007). With China emerging as a leader, research has shown that they are state funded and are training thousands of students in the area of hacking other government computers (Markoff and Barboza, 2010).

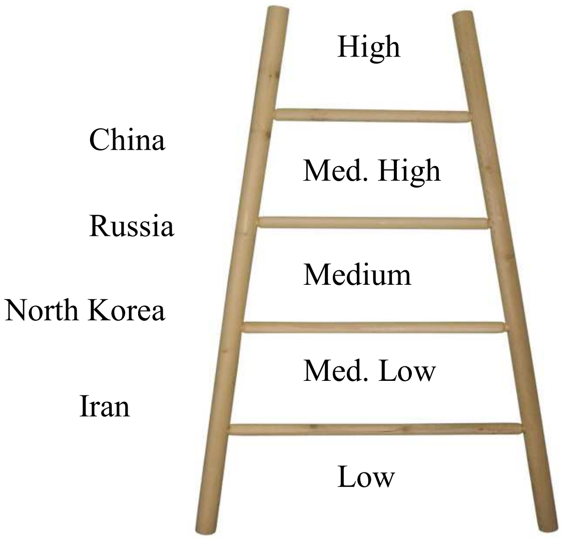
With cyber-tools constantly being changed, updated, or developed the use of methods such as steganography will continue to rise. The terrorist cells are finding newer, covert ways to communicate with one another in order to go unnoticed by the U.S. Those that are considered a threat to the U.S. are using covert methods because they are more difficult to trace (i.e. hiding information on a website or multimedia image or video) mainly because of the large number of every day users to sort through (Hosmer, 2012).

RECOMMENDATIONS

Ladder of Risk

The researcher showed what countries pose the greatest cyber-threats to the U.S. China was shown to be at the top of that list followed by Russia, Iran, and North Korea. There is still room for more research to help our government better understand what other countries are climbing the "ladder of risk" and why. The researcher recommends that agencies create a ladder of risk for potential threats and attacks alike. The ladder of risk should include steps for assessment starting with low risks and increasing at various increments. Note that a separate ladder should be created for who is a potential risk and what is a potential risk. Much like the Ryan-Nichols risk assessment equation, the ladder of risk is based on rating a risk at a certain level by taking the threats, vulnerabilities, and impact into consideration. Figure 9 below shows an example of a ladder of risk that an agency may want to implement using the four countries that pose the greatest risk to the U.S.

Figure 9: Ladder of Risk



Source: Adapted from: Trust Me It's Encrypted (Nichols, 2004)

As one can see from the example above, the ladder of risk would be used much like that of a risk assessment but can be incorporated in both physical and cyber-security realms. Any agency could use the ladder of risk to not only measure or classify the risk of a country but also to classify which steganography tools may be used more than others, which media is most likely to be used, and where covert communications may be hidden.

Assessing Cyber-Attack Threats

The damage of a cyber-attack (specifically steganographic attacks) can range from minimal to catastrophic. The U.S. should not focus on the largest or greatest threat they need to analyze a larger spectrum of various possible cyber-attacks and who can carry them out. "Every hacker knows that government and commercial computers can, accidentally or by design, disclose information that should be private. These susceptible areas of the U.S. computer systems are appealing to countries looking to cripple the U.S. Russia, Iran, and North Korea are more likely to plan attacks that threaten industrial trade secrets" (Simple Security, 2011).

The researcher recommends that agencies focus on what steganography tools are being used by cyber-terrorists in order to communicate with one another. Agencies need to triage which steganographic tools require pass phrases or just hiding the images without any encryption. Terrorists are currently using a multitude of steganography tools. With so many tools available one of the most commonly used tools is Steghide by Source Forge. Steghide is capable of hiding data in both image and audio files (i.e. jpeg, bmp, wav, and au files). The appeal of a program such as this is its open availability as well as the fact that it is considered freeware; therefore there is no out of pocket expense. PGE or Pretty Good Envelope is another example of a tool that is used by terrorists. This tool allows data to be hidden into GIF or JPG files making it easier to send them from a computer or even a mobile device. "S-Tools" is a tool being used by terrorists for communication based on its ease of use and ability to hide multiple files within one carrier file. QuickStego and QuickCrypto are two tools widely used for steganographic communications based on their abilities to hide and encrypt data. QuickStego will hide a covert message but will not encrypt the message. QuickCrypto will not only hide the information but it will encrypt it as well (CNET, 2012). Constant training forces agency personnel to stay up-to-date on exactly what steganographic tools and capabilities are used by terrorists.

Tools Analysis

It is also recommended that U.S. government agencies do further research on which tools can best protect their systems from steganographic attack and also detect possible steganographic messages on their networks. According to Gary Kessler, steganography is not detectable to the naked eye and tools today are becoming more advanced in their ability to elude steganography detection tools (Kessler, 2011). Currently there are over 100 tools available that have the ability to disguise information. It is recommended that the government implement the use of tools such as Stego Suite by WetStone Technologies. Stego Suite Tools encompass many programs in one allowing for better steganography detection. Stego Hunter detects the presence of steganography on a network. Stego Break allows investigators to obtain the "pass phrase" of a carrier file and also contains a password dictionary for use with dictionary attacks (WetStone, 2012). ***The best defense against steganography is a suite of software that has programs covering all aspects of steganography.***

Analyzing Media

The researcher showed the use of steganography to hide messages in various media types. The main carrier file types used are image based, however the researcher recommends that agencies investigate the possibilities of pictures, audio, and video files being used as a carrier file. Large image files are commonly used because of their size and their ability to hide larger messages. However, multimedia files are also used because of their ability to conceal audio messages within an already existing audio message and they can be used with mobile devices

Aside from the types of media being used the researcher recommends that further research be done on where the carrier files are being hidden or placed for retrieval. The researcher discussed the use of SPAM e-mail, regular e-mail, and web sites as locations that may be used to as a home for steganographic messages. It is recommended that internet auction sites and pornography sites be further investigated when searching for steganographic messages as they do not fit the common knowledge of what many possible cyber-terrorists believe in or practice. Many countries posing a threat to the U.S. have certain religious beliefs that would prevent them from using the aforementioned web pages, however, it is because of this that many may resort to placing their carrier files on such sites in the hopes that is will remain undetected.

AUPS

It is recommended that organizations use updated and thorough AUPs and network security policies to ensure the protection of their sensitive data. Current AUPs cover basic computer usage and access parameters; however, with all of the recent breaches in security new, improved, and more thorough security policies are necessary. The most current acceptable use policy for the DOD does not cover the use of steganography by terrorists as a method of communication. In fact, it is a policy encompassing who may use government "information systems" and how they may be used. It should be pointed out that the policy does make it clear to all users that transferring non-approved information and forwarding chain e-mail, suspicious e-mail, and virus warnings are not acceptable. Although the DOD's ***AUP does not deal specifically with steganography as a communication tool*** it does limit the user's ability to employ "hacker-related" software, sniffers, and interactive websites (i.e. Facebook, Yahoo Messenger, and MySpace) to maintain information integrity (DOD, 2012).

APPENDIX A

Glossary

AUP – Acceptable Use Policy; rules governing use of computers, networks, and associated resources (Department of Defense, 2012).

CIA – Central Intelligence Agency; an independent agency responsible for providing national security intelligence to senior US policymakers (Central Intelligence Agency, 2012).

Cryptography – the enciphering and deciphering of messages in secret code or cipher; also: the computerized encoding and decoding of information (O'Connor, 2011).

DOD – Department of Defense; provides military forces needed to deter war and to protect the security of our country (Department of Defense, 2012).

FBI – Federal Bureau of Investigation; protect and defend the United States against terrorist and foreign intelligence threats (Federal Bureau of Investigation, 2012).

Hacker – a person who illegally accesses and/or tampers with information in a computer system (Department of Defense, 2012).

Sniffer – a software or hardware tool that monitors data packets on a network to see if they arrive (Department of Defense, 2012).

Steganography – the art or practice of concealing a message, image, or file within another message, image, or file (Kessler, 2001).

APPENDIX B

Steganography Tools

Anti Steg	**Covert.tcp**	**Cryptix**	**CryptoPix**	**CryptoFlix**
Crypto	**Cipher Image**	**CoverText**	**dc_Steganograph**	**Dound's Steganography**
EzStego	**Eniledahs Secret Message**	**FFEncode**	**GzStego**	**Hermetic Stego**
Hide4PGP	**Hide and Seek**	**iStegano2005**	**Invisible Ink**	**iSteg**
MP3Stego	**MP3Stegz**	**Our Secret**	**Open Puff**	**PGE**
Picture Spy	**PGPn123**	**PictEncrypt**	**QuickStego**	**QuickCrypto**
Snow	**Stealth**	**Snow**	**S-Tools**	**Scytale**
Steg Break	**Steg Analyst**	**Steganos**	**Stego**	**StegHide**
Steg Watch	**Steg Hunter**	**Steganography**	**SecretPix**	**SpyPix for iPhone**
Texto	**Text Hide**	**wbStego**	**Wnstorm**	**Xiao Stego**

REFERENCES

Primary

Brenner, J. (2011). *America the Vulnerable*. New York, NY: Penguin Press.

Brenner, J. (2011). *Spies at Work Know Where to Find Your Secrets*. Retrieved January 19,

2012 from http://www.bloomberg.com/news/2011-02-11/spies-at-work-know-where-to-find-your-secrets-joel-f-brenner.html

Codr, J. (2009). *Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide*. Retrieved January 8, 2010 from http://www.cs.wustl.edu/~jain/cse571-09/ftp/stegano/index.html

Conway, M. (2008). *Code Wars: Steganography, Signals Intelligence, and Terrorism*. Retrieved January 5, 2012 from http://doras.dcu.ie/494/

Gaudin, S. (2001). *The Terrorist Network*. Network World; November 26, 2001;

Volume 18 pg. 48 Retrieved January 5, 2012 from

http://search.proquest.com.ezproxy.utica.edu/docview/215953927/134289A8FE24370289/1?accountid=28902

Hally, J. (2002). *Steganography: What is the Real Risk?* Retrieved January 31, 2012 from http://www.sans.org/reading_room/whitepapers/stenganography/steganography-whats-real-risk_555

Harris, S. (2008). *China's Cyber-Militia*. Retrieved January 28, 2012 from http://www.triprosec.net/pdf/china_cyber_militia.pdf

Hosmer, C. (08 February 2012). Private communication from subject matter expert.

Honeyman, P. & Provos, N. (2001). *Detecting Steganographic Content on the Internet*. Retrieved from http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

Judge, J. (2001). *Steganography: Past, Present, Future*. Retrieved January 19, 2012 from http://www.sans.org/reading_room/whitepapers/stenganography/steganography-past-present-future_552

Kellen, T. (2001). *Hiding in Plain View: Could Steganography be a Terrorist Tool?* Retrieved January 5, 2012 from www.sans.org/.../hiding-plain-view-steganography-terrorist-tool_551

Kessler, G. (2001). *Steganography: Hiding Data within Data*. Retrieved January 15, 2012 From http://www.garykessler.net/library/steganography.html

Kessler, G. (2001). *An Overview of Steganography for the Computer Forensics Examiner*. Retrieved January 12, 2012 from http://www.garykessler.net/library/fsc_stego.html#digitalcarrier

Kivento, T. (2006). *Technical Feasibility*. Retrieved February 18, 2012 from http://partnet.vtt.fi/evaserve/evaserve_tool/tech_feas/Technical_feasibility_v1.0.pdf

Nichols, R.K., Ryan, D.J., & Ryan, J.C.H. (2000). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves.* New York: McGraw Hill

Nichols, R.K. (2004). *Trust Me, It's Encrypted*." Retrieved January 8, 2012 from Professor Randall K. Nichols, Subject Matter Expert

Nichols, R.K. (2010). *INFOSEC and INFOWAR; Protection of Information Assets and Systems.* Retrieved January 16, 2012 from Professor Randall K. Nichols, Subject Matter Expert

Nichols, R.K. (12 January 2012) Private communication from subject matter expert.

O'Connor, T. (2011). *Cybercrime and Cybercriminals.* Retrieved February 4, 2012 from http://www.drtomoconnor.com/3100/3100lect03.htm

O'Connor, T. (2011). *Cyberterrorism and Cybervigilantism.* Retrieved February 12, 2012 from http://www.drtomoconnor.com/3100/3100lect04a.htm

O’Connor, T. (2011). *The Cyber Terrorism Threat Spectrum*. Retrieved January 30, 2012 from http://www.drtomoconnor.com/3400/3400lect06a.htm

O’Connor, T. (2010). *Disaster Data Recovery and Computer Forensics.* Retrieved February 4, 2012 from http://www.drtomoconnor.com/3100/3100lect08.htm

Orebaugh, A.D. (nd). *Steganalysis: A Steganography Intrusion Detection System*. Retrieved January 17, 2012 from http://www.securityknox.com/Steg_project.pdf

Owens, M. (2002). *A Discussion of Covert Channels and Steganography*. Retrieved February 19, 2012 from http://www.sans.org/reading_room/whitepapers/covert/discussion-covert-channels-steganography_678

Pope, L. (2008). *Cyber-Terrorism and China*. Retrieved February 17, 2012 from http://www.dtic.mil/dtic/tr/fulltext/u2/a490725.pdf

Provos, N. & Honeyman, P. (nd). *Detecting Steganographic Content on the Internet*. Retrieved January 24, 2012 from http://www.citi.umich.edu/u/provos/papers/detecting.pdf

Secondary

Astrwosky, B. (nd). *Steganography: Hidden Images, a New Challenge in the Fight Against Child Porn*. Retrieved January 28, 2012 from http://www.antichildporn.org/steganog.html

Ben-Ari, T. (2006). *Terror Spam and Phishing*. Retrieved January 31, 2012 from http://www.crime-research.org/articles/Terror-Spam-and-Phishing/

Center for Information Technology Integration (2002). *Steganography Press Information*. Retrieved January 29, 2012 from http://www.citi.umich.edu/u/provos/stego/faq.html

CNET Staff. (2009). Xiao *Steganography*. Retrieved January 31, 2012 from http://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html?tag=contentMain;contentBody;5d

CryptoPix. (2008). *CryptoPix Message Creator.* Retrieved February 18, 2012 from http://cryptopix.com/zform22.php

Dound's (nd). *Dound's Steganographer*. Retrieved January 31, 2012 from http://www.dound.com/Progs/Steg.htm

GmbH (2012). *Steganos Safe 2012*. Retrieved January 30, 2012 from http://www.steganos.com/us/products/data-security/safe/features/

Gorman, S. (2011). *China Hackers Hit U.S. Chamber*. Retrieved January 12, 2012 from http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html

GmbH (2012). *Steganos Safe 2012*. Retrieved January 30, 2012 from http://www.steganos.com/us/products/data-security/safe/features/

Gorman, S. (2011). *China Hackers Hit U.S. Chamber*. Retrieved January 12, 2012 from http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html

Johnson, R. (2011). *New Evidence Suggests China's Hacking Drones Using Adobe Reader and Internet Explorer*. Retrieved January 27, 2012 from http://articles.businessinsider.com/2011-12-22/news/30545577_1_virus-pdf-files-adobe-reader

Kelley, J. (2001). *Terror Groups Hide Behind Web Encryption*. Retrieved January 5, 2012 From http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

Lake, E. (2011). *China Deemed Biggest Threat to U.S.* Retrieved February 15, 2012 from http://www.washingtontimes.com/news/2011/mar/10/china-deemed-biggest-threat-to-us/?page=all

Lemos, R. (2011). 12 *Groups Carry Out Most APT Attacks*. Retrieved January 31, 2012 from 0http://www.informationweek.com/news/security/vulnerabilities/232300834?itc=edit_in_body_cross

M86. (2012). *Acceptable Use Policy and Compliance*. Retrieved February 15, 2012 from http://www.m86security.com/resources/acceptable-use-policy-and-compliance.asp

Markoff, J. & Barboza, D. (2010). *2 China Schools Said to Be Tied to Online Attacks*. Retrieved January 28, 2012 from http://www.nytimes.com/2010/02/19/technology/19china.html

Marquand, R., and Arnoldy, B. (2007). *China Emerges as Leader in Cyberwarfare*. Retrieved January 19, 2012 from http://web.mit.edu/gssd/cyberspace/Weekly%20Article/China%20emerges%20as%20leader%20in%20cyberwarfare.pdf

McCullagh, D. (2001). Bin *Laden: Steganography Master?* Retrieved January 5, 2012 from http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all

Mills, E. (2009). *Report: Countries Prepping for Cyber-war*. Retrieved February 17, 2012 From http://news.cnet.com/8301-27080_3-10399141-245.html

Radcliff, D. (2002). *Quick Study: Steganography: Hidden Data*. Retrieved January 7, 2012 From http://www.computerworld.com/s/article/71726/Steganography_Hidden_Data

Schneier, B. (2001). *Terrorists Hide Messages in Messages*. Retrieved January 17, 2012 from http://stacks.msnbc.com/news/633709.asp

Schwartz, M. (2011). *More Sykipot Malware Clues Point to China*. Retrieved January 31, 2012 From http://www.informationweek.com/news/security/attacks/232300940

Scorbett (2004). *The Science of Hiding in Plain Sight*. Retrieved February 18, 2012 from http://www.kuro5hin.org/story/2004/10/26/02313/946

Spam Mimic. (2010). Spammimic. Retrieved January 15, 2012 from http://www.spammimic.com/

Westphal, K. (2010). *Steganography Revealed*. Retrieved January 5, 2012 from http://www.symantec.com/connect/articles/steganography-revealed

WetStone Technologies (2012). *Stego Suite: Discover the Hidden*. Retrieved January 20, 2012 From http://www.wetstonetech.com/product/stego-suite/

Government

Department of Defense (2012). *AUP.* Retrieved February 6, 2012 from https://atc.us.army.mil/iastar/docs/aup.doc

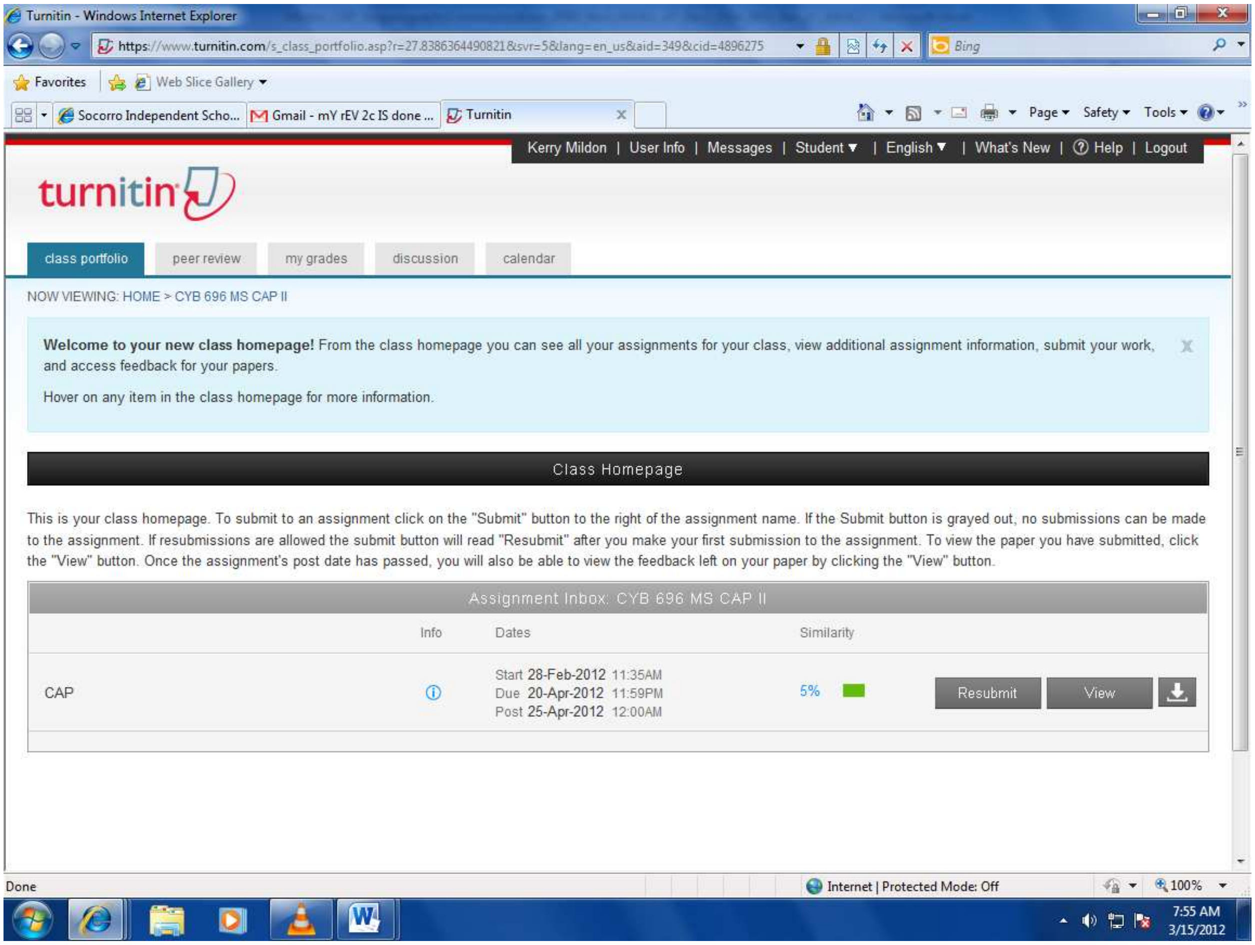
Federal Bureau of Investigation (2011). *FBI Counterintelligence National Security: A Blueprint For Protecting U.S. Secrets*. Retrieved January 20, 2012 from http://www.fbi.gov/news/stories/2011/november/counterintelligence_110411

Gray, P. (nd). *Protecting Privacy and Security of Personal Information in the Global Electronic Marketplace*. Retrieved February 16, 2012 from http://www.ftc.gov/bcp/icpw/comments/ico2.htm

Hovington, B. (2010). *Working with Communities to Disrupt Terror Plots*. Retrieved January 15, 2012 from http://www.fbi.gov/news/testimony/working-with-communities-to-disrupt-terror-plots

U.S. Army. (2012). *Computer-User Agreement*. Retrieved February 14, 2012 from https://atc.us.army.mil/iastar/docs/aup.doc

United States Institute of Peace. (2004). Cyber-terrorism: How Real is the Threat? Retrieved February 15, 2012 from http://www.usip.org/files/resources/sr119.pdf


Turnitin - Windows Internet Explorer
https://www.turnitin.com/s_class_portfolio.asp?r=27.8386364490821&svr=5&lang=en_us&aid=349&cid=4896275
Bing
Favorites
Web Slice Gallery
Socorro Independent Scho...
Gmail - mY rEV 2c IS done ...
Turnitin
Page
Safety
Tools
Kerry Mildon | User Info | Messages | Student ▼ | English ▼ | What's New | Help | Logout
turnitin
class portfolio
peer review
my grades
discussion
calendar
Done
Internet | Protected Mode: Off
100%
7:55 AM
3/15/2012

NOW VIEWING: HOME > CYB 696 MS CAP II

Welcome to your new class homepage! From the class homepage you can see all your assignments for your class, view additional assignment information, submit your work, and access feedback for your papers.

Hover on any item in the class homepage for more information.

Class Homepage

This is your class homepage. To submit to an assignment click on the "Submit" button to the right of the assignment name. If the Submit button is grayed out, no submissions can be made to the assignment. If resubmissions are allowed the submit button will read "Resubmit" after you make your first submission to the assignment. To view the paper you have submitted, click the "View" button. Once the assignment's post date has passed, you will also be able to view the feedback left on your paper by clicking the "View" button.

Assignment Inbox: CYB 696 MS CAP II

	Info	Dates	Similarity	
CAP	ⓘ	Start 28-Feb-2012 11:35AM Due 20-Apr-2012 11:59PM Post 25-Apr-2012 12:00AM	5% 🟩	Resubmit View