Research Paper on Internet Deception Tactics

PROFESSIONAL PROJECT

Michael J. Blair
November 13, 2006

Regis University
School for Professional Studies
MSCIS Program

Professional Project
Certification of Authorship

Student Name: Michael J. Blair
Course: MSC 696 Professional Project
Project Title: Research Paper on Internet Deception Tactics
Submitted To: Timothy McKenzie
Regis University
Date of Submission: xxxx xx, 2006

CERTIFICATION OF AUTHORSHIP: I certify that I am the author of this project and that any assistance I received in its preparation is fully acknowledged and disclosed in the paper. I have also cited any sources from which I used data, idea or words, either quoted directly or paraphrased. I also certify that this paper was prepared by me specifically for this course.

______________________________
Michael J. Blair
Advisor/MSC 696 Faculty Approval Form

Student Name: Michael J. Blair
Professional Project Title: Research Paper on Internet Deception Tactics

Advisor’s Declaration: I have advised this student through the Professional Project process and approve of the final document as acceptable to be submitted as fulfillment of partial completion of requirements for the MSC 696 course. The student has received project approval from the Advisory Board and has followed due process in the completion of the project and subsequent documentation.

ADVISOR
Printed Name __________________________ Signature ____________ Date ____________

MSC 696 Faculty Approval

Printed Name __________________________ Signature ____________ Date ____________
Abstract

The conception of the Internet was to provide geographically separated units with a mechanism to transfer research information. The use of the Internet to identify, track and apprehend cyber criminals by investigators has increased following the events of 9-11. It is publicly known that criminal organizations both foreign and domestic utilize the Internet to solicit, support and direct followers to carry out and plan criminal activities. Criminal and terrorist organizations now have a powerful tool, a global command and control system capable of teaching, funding, organizing, and executing criminal/terrorist ideology. Deception has been used for years as a mechanism for criminals to conduct unlawful acts. Today, criminals and terrorist organizations are using the art of deception to expand their criminal empire globally via the Internet. The following research paper will explore how the Internet has become a breeding ground for deceptive tactics and a command and control mechanism for criminal and terrorist organizations.
# Table of Contents

Abstract .......................................................................................................................... 4  
1.1 Introduction ............................................................................................................. 7  
1.2 The Art of Deception ............................................................................................ 7  
1.3 Lessons of Nature .................................................................................................. 8  
1.4 Deception in Human History ................................................................................. 9  
1.5 WEB of Deception ................................................................................................. 10  
2 Research and Analysis ............................................................................................... 13  
2.1 Deception Techniques/Tactics ................................................................................. 13  
2.2 Phishing / Pharming ............................................................................................... 13  
   2.2a Techniques to Mitigate Phishing Schemes ......................................................... 20  
2.3 Spyware .................................................................................................................. 26  
   2.3a Techniques to Mitigate Spyware ......................................................................... 27  
2.4 Spam ...................................................................................................................... 29  
   2.4a Techniques to Mitigate SPAM ............................................................................. 30  
2.5 Malware ................................................................................................................. 32  
   2.5a Techniques to Mitigate Malware ......................................................................... 35  
3.0 Crime on the Global Information Grid .................................................................... 36  
3.1 Web and the Mob ................................................................................................... 36  
   3.1a High Tech Crime Fighting ................................................................................... 37  
3.2 Economic Espionage .............................................................................................. 41  
3.3 Terrorist Online ..................................................................................................... 48  
   3.3a Planning and Coordination ................................................................................ 49  
   3.3b Encryption ........................................................................................................... 50  
   3.3c Propaganda ......................................................................................................... 52  
4.0 Lessons Learned .................................................................................................... 55  
5 References .................................................................................................................. 58
1 Introduction and Background

1.1 Introduction

Technological developments over the past decade have made deception a key element in asymmetric warfare weapon systems. Advances in military stealth technologies allow aircraft the ability to conceal its identity on radarscopes by appearing to be a small bird. The ability to maintain concealment provides stealth aircraft the ability to execute mission requirements while being undetected.

Computer experts and Hackers utilize deceptive tactics to conceal and deceive online users about their personal information such as geographic locations, IP, MAC and Email address by using deceptive tactics and stealth technology. Federal investigators are able to utilize these same deceptive tactics to apprehend criminals, such as child molesters, child pornography rings and online organized crime groups. The concept of deception has been used for centuries by man and nature to trick unsuspecting adversaries. The following pages will explore how the concept of deception is used by Hackers, Organized Crime Organizations, Terrorists and Federal Investigators on the World Wide Web to achieve crime and trickery.

1.2 The Art of Deception

“In late 1990, before the start of Operation DESERT STORM, U.S. amphibious training was conducted in the Persian Gulf. The training demonstrated the US forces’ amphibious capability, as well as US and Coalition resolve concerning the crisis. Inevitably, journalist asked if an amphibious
invasion was planned. In keeping with operational guidelines for discussing information with the media, military officials would not comment on future operations. Even though an amphibious landing ultimately was not conducted during Operation DESERT STORM, Iraqi perception of the US and Coalition capability and resolve may have caused them to conclude that an amphibious invasion was likely. As a result of their perception, Iraqi forces may have focused additional attention and resources that could have been employed elsewhere to defend against an amphibious invasion that never materialized" [AF Doctrine 2-5).

1.3 Lessons of Nature

The art of deception has been around for centuries and studied throughout history as a tool or weapon designed to deliberately mislead ones opponent into believing or perceiving an event to be true. One can learn a lot about deception, and how it can be used as a defense mechanism, by studying the deceptive techniques of nature. Biologists for years studied how certain techniques have enabled species to survive by tricking predators. A well-known technique is the ability for animals to camouflage themselves in their environment by pretending to be an inanimate object. The butterfly can change its colors to deceive predators into believing it is a leaf. An insect such as the walking stick utilizes cryptic coloration to pretend to be a twig on a tree to avoid being seen by a bird or other predator. The African devil flower looks like an appetizing flower, with fake flies to lure insects to its deadly petals (Epstein, 2003). These are just a few examples of how deceptive tactics are vital to survival in the wild. An important
point to consider is that deception is not only used by predators but by prey as well.

1.4 Deception in Human History

“Warfare is the way of deception”, Sun-Tzu

The art of deception in our history is abundant with stories and legends of deception. Deception can be tracked back to 4th Century BC when Sun Tzu advocated the use of guile and deception to overcome one’s enemy. Conventional wisdom suggests that the use of deception in war is not to increase your opponent’s casualties of war, but to win the war without even fighting the war. As described in the example at the beginning of this chapter, deception can provide a distraction to our adversaries’ attention from legitimate friendly military operations, and can confuse and dissipate adversary forces. [AF Doctrine 2-5]

A well-known use of military deception is the Trojan horse used by the Greeks. The Greeks constructed a large wooden horse in 1183 B.C. as a mechanism to hide warriors inside and breech the formidable gates of Troy. The Trojans believed that the Greeks had conceded their ten-year siege, and took the horse into the city as a token of victory. While the Trojans celebrated victory the Greeks emerged from the horse and opened the gate of Troy to thousands of awaiting Greek warriors.

Deception can be seen in biblical scriptures in Genesis 3:1-7 when Satan the master of deception intentionally lies to Eve in order to deceive her by explaining that the tree will bring knowledge by eating the forbidden fruit and God was attempting to keep something desirable from her and Adam. The ability of
Satan to persuade Eve into believing something that was not true is an excellent example of how humans are easily manipulated, by the desire for power and knowledge, into believing things that are untrue.

1.5 WEB of Deception

The use of computers for business and pleasure has created a surge of electronics into the mainstream population. With every innovated idea there is always a mechanism that tries to destroy the integrity of the original design. The Internet, which was originally designed to provide geographically separated research facilities the ability to share intellectual information, has now become a breeding ground for deceptive behavior. Online users are now victims of identity theft, fraud, and vulnerable to hundreds of malicious codes, such as viruses, worms, phishing, spyware, and annoying spam. The United States Government Accountability Office conducted a study and concluded, “Spam, phishing, and spyware, while once viewed as discrete consumer challenges, are being blended to create substantial threats to large enterprises, including federal systems. According to security researchers and vendors 2004 annual security reports, phishing and spyware were identified among the top emerging threats of last year, and they are predicted to increase in 2005”. [GAO, 2005] According to the FBI, international crime cells, such as terrorist, transnational criminals, and intelligence services are starting to use information exploitation tools such as computer viruses, Trojan horses, logic bombs, and eavesdropping sniffer to degrade the integrity of or deny access to sensitive economic and commercial
In May of 2005, the Internet Fraud Complain Center (IFCC) released a spam fraud alert for cyberspace users. The press release information states that spammers are trying to capitalize on the popularity of the Pope's death to promote a moneymaking scheme. The spam email deceives people into believing they can receive free books about the Pope by clicking onto the link attached to the email. Once the link is clicked on users are redirected to a website that advises them that the books are not available, again the user is redirected to another website that provides money investment secrets and mentions nothing about the Pope.

Another Internet crime complaint listed on the IFCC website identifies a credit/debit card harvesting scam. Cyberspace users are receiving emails advising them that they have won a Microsoft X-Box. The email instructs the user to click on the attached website link. Once on the site the website requests that the user place their debit card account number and personal identification number to pay for shipping and handling charges. Users who have become a victim to this scam have advised law enforcement officials investigating this complaint that their debit accounts are getting charged more then the original shipping costs and the user never received the X-box (IFCC, XXXX).

The use of the Internet by terrorist organization has become a huge concern for law enforcement agencies trying to isolate, deter and destroy this global menace. Due to the openness and ease of use, the Internet has become
the major tool for spreading propaganda and deception by Islamic extremist. Al-Qaeda has requested that its supporters download articles from their sites and disseminate them via their own web sites, discussion forums and email lists. This will provide continuity in their propaganda efforts because as law enforcement authorities close one site another is opened with the same information as the latter. [ADL 2002]

Cyberspace has also provided charitable organization a valuable mechanism to solicit financial support for their organizations. This provides the humanitarian organization with an excellent marketing tool. As mentioned previously it does not take long for someone to take the ingenuity of a concept and destroy the integrity of its original design. Law enforcement agencies have been able to identify online humanitarian foundations such as the Benevolence International Foundation (BIF), the Global Relief Foundation, and the Al-Haramain Foundation, linked to fund raising and money laundering for Al-Qaeda cells operating in the United States. The BIF foundation deceived contributors into thinking they were funding humanitarian efforts to help those individuals afflicted by wars. The foundation site provided investors with the option of making a contribution with a credit card, instructions on how to wire money, a form to provide a monthly contribution automatically from your bank account, and most notably how you can donate stocks. [ADL 2002]
2 Research and Analysis

2.1 Deception Techniques/Tactics

As presented it is easy to comprehend how simple it is to deceive people who are unaware of the risks associated with cyberspace crime tactics. The following section will provide an understanding of the various types of criminal tactics currently used on the Internet. The following chart was created by the GAO and details the sources of emerging cyber security Threats.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishers</td>
<td>Individuals or small groups that execute phishing scams in an attempt to steal identities or information for monetary gain.</td>
</tr>
<tr>
<td>Spammers/Spyware</td>
<td>Individuals or Organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing scams, distribute spyware, or attack organizations (i.e. Denial of Service)</td>
</tr>
<tr>
<td>Malware</td>
<td>Is an abbreviation for malicious software and is crafted specifically to damage or disrupt electronic systems.</td>
</tr>
<tr>
<td>Criminal Groups</td>
<td>There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain; further, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud.</td>
</tr>
<tr>
<td>Foreign Intelligence Services</td>
<td>Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities.</td>
</tr>
<tr>
<td>Spyware/malware authors</td>
<td>Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.</td>
</tr>
<tr>
<td>Hackers</td>
<td>Hackers sometime break into networks for the thrill of the challenge or for bragging</td>
</tr>
</tbody>
</table>

Source: GAO

2.2 Phishing / Pharming
The deliberate use of the Internet to steal consumers’ personal identity and financial account credentials is known as phishing or pharming. These types of attacks are known to use social engineering and technical subterfuge to launch their attacks. The use of social engineering utilizes spoofed emails to direct users onto counterfeit websites and tricks recipients into divulging financial data, such as account user names, passwords and social security numbers, as well as credit card numbers (McAfee, 2006). The attackers are able to hijack websites from legitimate businesses to support their phishing schemes. A recent phishing scheme targeted the South Trust bank website in November 2005. An email was sent out to account holders advising them to confirm/update specific account information by simply clicking on the attached Web link. The banks' original URL is provided but the hyperlink is spoofed to the hacked website. Once on the spoofed site unsuspecting users provide personal account information, such as Personal Identification Numbers (PIN), account passwords, social security numbers and other confidential information.

As I was writing this research paper I had the opportunity to become involved in an eBay Phishing Scheme. I was perusing the Ebay motors specialty site looking for an old Chevrolet Pickup truck for a good price. Unfamiliar with how the bidding process worked I jumped into a bidding war for a restored 1971 C10 pickup. My final bid was $7,500.00 and I was the highest bidder but the Reserve (the minimum the seller will release the merchandise to a buyer; if the reserve is not met then the seller is not obligated to sell) was not met. The next day I received an email from the purported seller indicating that he was willing to
sell the vehicle to me for my highest bid of $7,500.00. I was truly excited because this was going to be a good deal and I continued to discuss the specifics of the transaction with the seller. While away on business we continued communicating over email and advised the seller I could not close the deal until I arrived back home from my business trip. The seller assured me he would wait and to contact him when I got back in town. We continued to discuss specifics and I asked a question on how the truck would be shipped and the additional cost I would incur (the buyer is responsible for all shipping costs associated with claiming the merchandise). The seller sent an email back stating the shipping cost was already included within the sale price and there would be no additional cost. Again I was taken back that this was too good to be true. The seller advised me that his son works for Lufthansa Cargo Company and he gets a 60% discount on all cargo shipments and the remaining 40% was included within the sell price. After a short deliberation on the explanation provided, I again put myself at ease and felt reassured about the impending business transaction. I arrived back home and contacted the seller via email requesting he send the eBay sellers transaction report detailing the vehicle, cost and payment options. The seller advised me he notified eBay about the transaction and should receive a document from eBay detailing the sale. Within the same email he mentioned he was out of town on business and I could wire (Western Union) the money to his present location to expedite the shipping of the vehicle. I received the information from eBay and it provided me with a hyperlink and picture of the truck being purchased (exhibit 1).
I decided to review the truck options one more time and clicked on the link to see additional pictures. The hyperlink brought me to a different vehicle. I emailed him back and advised the sale transaction from eBay brought me to a totally different vehicle and I did not feel comfortable going through with the transaction.
The seller emailed me back and mentioned an updated transaction document from eBay should be sent in about a half hour. Within 15 minutes a new updated eBay seller report with a hyperlink to the correct vehicle information, but now the sellers information was different from the original. The seller explained that since he was out of town I could wire the money to his business partner listed on the second sheet (exhibit 2).

Exhibit-2

[Email message]

Re: C10

From: Fno222
To: MLSAIR19709

I have the transaction document that you reported and have sent to [Redacted]. I will get the updated items so you can review the transaction information. The updated transaction document from eBay should be sent to you in about a half hour. Within 15 minutes a new eBay seller report with a hyperlink to the correct vehicle information, but now the sellers information was different from the original. The seller explained that since he was out of town I could wire the money to his business partner listed on the second sheet (exhibit 2).

Now being totally confused about the whole transaction I decided to speak to the seller and requested a telephone number. While waiting for a response I performed an online Internet directory assistance on the first name provided by the original eBay transaction report (the purported seller name). A query on the
name, city and state provided me with a street address that matched the sellers eBay information and a telephone number. I called the number not expecting the person to answer since he was out of town on business. A gentleman answered the phone and I asked if this was Albert Clark, at address provided.

The man replied, “Yes that’s me.”

I said, “Hello Albert this is Mike we have been communicating online about the C10 pickup truck on eBay.”

He said “Son, you are about the 10th person that has called me about the truck and I don’t have a truck for sale nor have I ever been on eBay.”

Relieved and concerned I contacted the eBay security center and forwarded them the correspondence information. Within a few minutes I received an email message back advising me not to engage in any further discussions because the information provided is coming from a fraudulent website unaffiliated with eBay. Long story short, I felt like I won the lottery, my wife was now talking to me because I did not spend $7,500.00 and even cooked me dinner because I did not get suckered into a spending something for absolutely nothing.

A more sophisticated phishing technique is technical subterfuge. Internet users will visit Web sites that have been set up to deploy key logging Trojans. Once on the users computer, the Trojan waits for the user to visit his or her bank’s Web site. The keylogger captures all of the keystrokes when a user signs into their account. The information is then harvested back to a site where the hacker retrieves the information. Pharming uses a device installed on the users’ pc to misdirect personal information from fraudulent sites [APWG, 2005].
Phishing schemes are reported as an increasingly popular scam and the Anti-Phishing Working Group reported that 17,000 fraudulent attacks were launched in November 2006 alone (Leyden, 2006).

The following screen captures shows a PayPal phishing scheme.
2.2a Techniques to Mitigate Phishing Schemes

Technology experts and law enforcement officials are researching ways to deter and combat email Phishing Schemes. The latest statistics taken by Anti-Phishing Working Group (Antiphishing.org) as of March 26, 2006, depicted below details the continued increase of reported phishing crimes.

The following Graph provided by the Anti-Phishing organization depicts the countries hosting Phishing Web-sites. Currently the United States is at the top with %36.57 of the pie.
Experts agree that in addition to continued end-user education awareness there is also a need for mail transfer agent (MTA’s) technical solutions that are proven and cost effective to implement and maintain. Tumbleweed Communications published a white paper detailing some innovative techniques to help prevent and or reduce the number of phishing schemes. Listed below is a brief technical review of the proposed solutions detailed in the report:

1. **Sender Policy Framework (SPF)**

   This solution was developed and engineered by Meng Weng. The SPF system uses the TCP/IP connection from the originating MTA...
(Email Server) and compares this to IETF organizationally assigned IP addresses stored within a DNS server located at the recipients ISP or Corporate DMZ. If the sending IP address does not match an organizationally assigned IP address during DNS query the email is discarded or local network security policies dictates how this incident will be handled. If the query comes back and the IP address can be authenticated the email is delivered to the recipient.

Depicted below is a diagram provided by Tumble Weed detailing how the email traffic flow would work in the SPF environment.

The advantages to utilizing this approach is that the cost to maintain an updated DNS list is free and organizations can independently register their authorized IP address in DNS at no charge. The disadvantage to
utilizing this architecture is both sides of the network (Sender & Recipient) have to support SPF for the connection to work. There are approximately a few hundred thousand Internet emails but only 8,000 of them have SPF entries (Tumbleweed, 2004).

2. Microsoft Caller-ID

The Caller-ID conceptually looks and feels like the SPF authentication solution. The sender of e-mail reports, or publishes the assigned IP address of their outgoing SMTP mail server in the Domain Name System (DNS) with an e-mail policy document. The receiving e-mail server queries the DNS for the e-mail policy and determines the “purported responsible domain” of the message. The authentication or comparison of the DNS against the originating e-mail provides the integrity check for the recipient (Tumbleweed, 20004). Depicted below is Tumbleweeds conceptual of how MS Caller-ID process flows:
The advantage to using Caller-ID is that each organizational mail domain can register their authorized IP address to DNS free of charge. The purported responsible address verification process provides a more in depth analysis to authenticate senders. Phishers who attempt to use spoofed purported responsible addresses will be dropped immediately by the MTA performing the Caller-ID check (Microsoft, 2004).

The disadvantage to using Caller-ID is that each network must support the connection to work (Tumbleweed, 2004).

3. **Asymmetric Cryptosystems or Public-Key Infrastructure (PKI)**

PKI policy utilizes user names, network addresses and trust levels to authenticate and grant network resources to allow users the ability to read and send emails. A user is then provided a public key (randomly
generated prime number) via certificate. A certificate is an electronic
document that contains the name of the owner of the key, the time
period or validity of the certificate, and the owner’s public key. The
owner’s ticket is then electronically signed by a trusted authority called
a certificate authority (CA) (Tumbleweed, 2004).
The public and private keys are always used together to encrypt and
decrypt messages. A user has the capability to share their public key
with other users to encrypt a message destined for that user. When
the user receives an encrypted message, they then can decrypt the
message using their private key. To assist mail delivery to users who
do not possess your public key they can communicate with a trust
agent or a MTA (certificate server, revocation lists) to retrieve the
public key. The following details how an email using the PKI encrypted
message system:

a. Step 1: The sender of the email will contact the recipients
directory server to obtain the recipient’s public key.

b. Step 2: The sender will then download the recipients certificate
and perform a validation of the certificate used. For instance
check the certificate against published revocation lists and also
validates certificates signing chain.

c. Step 3: Once the recipient’s certificate has been validated the
sender will extract the recipient’s public key and use it to encrypt
the message.

d. Step 4: Once the message has been encrypted it is then sent
or forwarded to the recipient.

e. Step 5: The recipient will receive the encrypted message and
then decrypt it using their own private key.
The disadvantage to this system is the complexity and administrative overhead to manage this type of system. If a company does not maintain an up to date certificate server it would be difficult for the sender to find a recipient’s certificate on the server. If a client’s MTA (certificate server or certificate authority) is not online, the PKI system cannot perform the required functions to encrypt and decrypt messages.

2.3 Spyware

Spyware is a broad term used to describe various software and applications that harvest information about a user’s online habits and reports it back to the creator. The behavior of spyware can range from annoying pop-up ads, browser hijacking and more advanced techniques such as theft of personal information, keystroke logging, changing of ISP phone numbers to expensive toll numbers and installing a backdoor into your system for awaiting hackers. Spyware and other potentially unwanted programs (PUPs) are wreaking havoc on corporate networks by degrading productivity by consuming bandwidth and affecting network performance and exposing confidential information (McAfee, 2003).

“Spyware is threatening the core concepts of data security, confidentiality, integrity and availability (CIA) of federal computer systems by capturing and exposing sensitive data, making unauthorized system changes, decreasing system performance, all without users knowledge or consent” [GAO, 2005].

Listed below are examples provided by [APWG, 2005] of three types of spyware:
• **Drive-by-downloads**: this type of spyware requires no permissions or interaction with the user at all. The application is loaded onto the users' computer when he visits a website, opens a zip file, or clicks on a malicious pop-up ad.

• **Spying**: this type of spyware is simply designed to capture information on the surfing habits for marketing purposes. The disturbing part is the invasion of privacy one feels. Information obtained from these marketing tactics includes the user's hostname, IP address, login names, passwords and keystrokes.

• **Keyloggers**: this type of spyware installs an application that monitors the user's keystrokes and then sends the information back to the creator. The application can install an email proxy on the target host and have the information emailed or logged on a server. Listed below are the various types of keyloggers:
  
  o **Hardware Keylogger**: a device placed between the keyboard and the computer. This type of spyware requires physical access to the machine and has the power to capture hundreds of keystrokes.

  o **Hooking Mechanism**: this logging is accomplished by using the Windows function SetWindowsHookEx() that monitors all keystrokes. The software is typically packages with an executable file that initiates the hook function and a DLL file to handle the logging function.

  o **Kernel / driver keyloggers**: this keylogger operates at the kernel level and receives data directly from the input device (keyboard). The disadvantage to this approach is that it fails to capture auto complete passwords.

### 2.3a Techniques to Mitigate Spyware

The first step to prevention is the ability to recognize the signs of spyware on your computer system. For most users the signs of spyware running on their computers is a noticeable difference in system response time. Typically when multiple spyware programs are running behind the scenes on your computer the performance appears to be sluggish and noticeably slow. Other signs of
spyware are annoying pop-ups or junk mail from a website that was previously visited.

One way to prevent cookie-based trackers from snooping your computer habits is to simply opt out of their services. For example, a popular spyware marketing firm provides users the ability to opt out of unwanted advertisements popping up in your browser. Users can click on Double Click Cookie OPT Out and select to no longer receive spyware cookies from Double Click supported websites.

To assist in finding other spyware cookies or programs running on your computer a software-based solution can be implemented. There are numerous freeware programs that home users can use to assist in mitigating these types of programs. A popular freeware is Spyware Search and Destroy version 1.4. This program detects and eradicates stealth spyware and protects computers from over 400 different types of spies.

Additionally another way to minimize risk and prevent unwanted cookies to be loaded is to become familiar with the various security settings on your Internet browser. For example, in Internet Explorer under the Internet Options from the Tools menu select the Privacy tab. Users are able to adjust the level of privacy wanted for your browser. Most users set the level of privacy to medium, but have the ability to move it to a more secure setting. The disadvantage to setting the privacy button to high is that some websites will become inoperable because certain cookies need to be active or loaded before the site can be seen (McAfee, 2005).
2.4 Spam

Unlike ham, which is e-mail that online users want, spam is characterized as unsolicited e-mail on the Internet. Spam is a form of junk mail that is sent out electronically to a large email listing. The large email listings are the result of a spambot program that collects e-mail addresses from the Internet. The spambot program can collect email addresses from Web sites, newsgroups, and special interest groups as well as chat room conversations (TechTarget, 2000).

Spammers are becoming more and more intrusive with their efforts to send out electronic junk mail. Hackers are now using war-driving to perform drive-by-spamming to gain access to unsecured wireless networks. This method provides spammers with an unlimited amount of bandwidth at no costs and also provides them with a level of covertness due to the difficulty to tracing spam back to the source (TechTarget, 2003).

The overhead that computers use to process this unsolicited information causes system resources to be bogged down. A noticeable difference can be seen in the network performance due to the back end system resources processing of unsolicited email. For example, legitimate email messages must now wait for SPAM to be processed by the MTA before mission critical information can be processed. The slowness in the network is more apparent if the current network infrastructure is already operating at peak performance. From a small business perspective, a network with 50-100 users, the amount of SPAM received and processed can cause huge production problems. The disk
space on an Exchange server could be an issue. It's not that users are deliberately saving SPAM emails but some organizations are required to archive deleted emails for a year or more. The following is a description of a SPAM problem within a small business setting.

“I recently helped a friend who owns a trucking company deal with a SPAM problem in their organization. The organization was receiving so much SPAM that it was becoming difficult to even use E-mail. Each user was receiving dozens of messages every hour. The real problems started when the company received an outrageously expensive phone bill. One of the users had apparently opened a message containing a malicious script that caused the PC’s modem to dial a 900 number. In the end, I was able to get rid of the dialer, but the SPAM problem had grown so far out of control that everyone in the company had to get a new E-mail address. Of course that meant informing all of the clients of the new contact information.” (Posey, 2003)

2.4a Techniques to Mitigate SPAM

Some businesses are starting to see the benefits in outsourcing their SPAM protection program to a third party. For example, a third party vendor provides an organization with up to date SPAM filters to combat the latest and greatest techniques used by marketing schemes. The cost savings for outsourcing this program helps reduce the need for costly hardware and software investments. Outsourcing an organization can potentially eliminate the extra cost to hire and train a support staff to track and monitor this program internally. This type of solution allows business owners the ability to see results on their
investments faster, because the migration is typically engineered to seamlessly integrate into an existing network architecture. A recommended third party solution is Message Labs Ltd. This company provides Anti-Spam services to small and large organizations and boasts a service level agreement (SLA) guaranteeing a SPAM capture rate of 95%.

A second option would be to install a software based solution offered by McAfee or Symantic. McAfee SpamKiller for Mail Servers application provides an added security and email-filtering device to stop SPAM at mail servers. The application provides system security administrators with the ability to filter on SPAM, phishing and inappropriate content (McAfee, 2006). The application will scan all inbound email traffic for these types of messages and immediately delete or quarantine message traffic to a junk e-mail folder.

The benefit of using this type of tool provides additional space on email servers, and increased employee productivity. Additionally, there are no hardware infrastructure changes needed to be made. The application can be loaded right onto your MS Exchange or Lotus Domino servers. There is no need to re-route mail through a third party or a hardware appliance. The disadvantages to this approach are that the mail is checked once it is at your exchange server. If the mail is routed through a sendmail server or something similar the SPAM mail is still being handled by your network and the overhead may decrease network performance.

The third option would be to install a network appliance to scan all inbound mail before sending it on to the internal messaging systems. The email
appliance will provide initial content filtering for all email traffic destined to the internal network. There are many vendors who offer these types of appliances, such as CipherTrust IronMail and Mirapoint RazorGate.

2.5 Malware

Spam is considered by many as an online nuisance. This nuisance is now capable of providing a delivery mechanism for malicious software programs (commonly referred to as malware) that hijack computers (GAO, 2005). The correlation between Spam and Malware is malware-laden messages are typically unsolicited and sent in bulk to end-users. Malware is defined as any software programming intended to cause harm. These programs can be identified as viruses, worms, spyware, and Trojan horses. The damaging effect of these programs can corrupt files, alter or delete data, disable hardware, harvest and distribute compromised confidential information, and most notably create a denial of service situation.

A virus is a computer program, or scripts that are capable of replicating across computers and networks to alter data or files. A computer virus is similar to a human virus because they are spread from an infected person to a non-infected person. The severity of the human virus can be as simple as an annoying cough or runny nose to more severe effects such as high temperature, sore throat, and muscle aches, ultimately resulting in loss of time at work. A computer virus can also have varying degrees of annoyance or severity. For example, the computer would not get a cough but could have an annoying pop up advertisement that is manageable but comes and goes. A more severe
symptom would involve damage to the computer hardware, software, or files causing loss of work time. A computer virus typically requires some action by the end user, such as clicking on an email attachment or downloading from an infected FTP site. The user is duped into thinking that the files come from a trusted source. The computer virus is sent from one computer to the next by sending an infected file, email or attached to another person. The computer virus is spread unknowingly to the next person, until a symptom has been noticed, such as a cough (annoying pop up) or more severe symptoms such as a sore throat or high fever (programs running slow, hardware failure).

A WORM is an acronym for write once, read many which is an optical disk technology that allows users to write data onto a disk just once and have the ability to ready this information any number of times. The worm is considered a variant of a computer virus and the only difference is that a worm can spread from one person to another without any interaction. A worm can be considered a pandemic because it has the ability to replicate itself on a computer system and send out hundreds of thousands of copies of itself. Worm variants are known to infect e-mail address books and systematically send out emails to everyone on the contact list and once received by the target host the worm can continue to infect the receiver’s e-mail address book and the cycle continues. Typically worms do not alter files and reside in active memory, which allows the program to act covertly until the replication process consumes system resources and dramatically slows other system tasks (McAfee, 2006). Worms are known to
consume network bandwidth and not allow network resources to respond to end users' requests.

A Trojan Horse is defined as a malicious code that is covertly hidden within programming or data to gain control of the system and perform malicious activity. The name Trojan horse comes from the story depicted in the beginning of this paper on deceptive tactics. A computer Trojan appears to be a useful software program but once the user lets the software program into its file system the damage begins. Users are deceived into believing the software file or program they are installing is legitimate and coming from a trusted source. The severity of a Trojan horse can be minor (such as adding a desktop icon or changing the background on your computer screen) to more severe results (such as deleting files or deliberately destroying system databases). More sophisticated Trojan Horse programs covertly install a back door into the infected computer and allow hackers the ability to access confidential or personal information.

Browser hijackers are programs that are capable of altering your computer's browser settings that systematically redirect users to alternative Websites other than what was requested. These types of programs are typically the result of a freeware installation and the user agreement has stated in the fine print that the program will install a browser hijacker when installed. The problem is users see the fine print, give it a quick look over and do not see the part where a browser hijacker will be installed. The damaging effect of a browser hijacker is the ability to add bookmarks to unsolicited Websites such as pornographic pop-
up windows or redirect the user homepage to an illegal Website. Michelle Delio, a writer from Wired.com, reported the following browser hijacking incident:

"The police raided my house on Sept. 17, 2002," said "Jack," who came to the United States from the former Soviet Union as a political refugee, and has requested that his name not be published. "Nobody gave me a chance to explain. I was told by judge and prosecutor that I will get years in prison if I go to trial. After negotiations through my lawyer I got 180 days in an adult correctional facility. I was imprisoned for 20 days and then released under the Electronic Home Monitoring scheme. I now have a felony sex-criminal record, and the court ordered me to register as a predatory sex offender for 10 years."

Jack originally believed that the images found on his computer were from a previous owner -- he'd bought the machine on an eBay auction. But he now thinks a browser hijacker may have been responsible.

"When I used search engines, sometimes I got a lot of porn pop-ups," Jack said. "Sometimes I was sent to illegal porn sites. When I tried to close one, another five would be opened without my will. They changed my start page, wrote a lot of illegal porn links in favorites. The only way to stop this was turn the (computer's) power off. But when I dialed up to my server again, I started with the illegal site, then got the same pop-ups. There were illegal pictures in pop-ups."

**2.5a Techniques to Mitigate Malware**

Users are able to combat these types of deceptive tactics by simply following these steps:
• Always ensure that your computer system is running the most up to date software patches on a regular basis. These updates should include your operating system as well as your anti-virus software application.
• Only download from reputable file transfer sites and software vendors.
• Always weigh the risk and benefits before installing something on your system and be aware of any user agreement “read the fine print”. A simple way to review this would be to do a search on the user agreement on browser hijacker.
• Install and always use a firewall topology, whether in your home or office.

3.0 Crime on the Global Information Grid

3.1 Web and the Mob

Organized criminal groups now poised to expand their criminal empires across continents have found the need to understand how to utilize the Internet to remain competitive and maintain a certain level of influence over their criminal empire. Criminal organizations have discovered that the Internet can provide new opportunities and multiply benefits for illicit business. The motivation goes beyond fraud and extortion and provides criminal organizations the ability to covertly maintain surveillance of law enforcement, enhance money laundering techniques, share pervasive pornography, develop and conceal pedophile rings, organize drug trafficking and most importantly a tool for secure and anonymous communication. The Internet provides an avenue for various kinds of theft, such
as robbing online banks or illicitly gaining intellectual property (Williams, 2002). The use of online auctions and gambling provides a mechanism to launder money through seemingly legitimate purchases, simply by paying more than the goods are worth. Online gambling also makes it possible to move large amounts of cash to offshore financial centers (Williams, 2002). In September 1999, two members from the group known as “Phonemasters” were convicted for penetrating computer systems of MCI, AT&T, Sprint and Equifax. The pair downloaded thousands of calling card numbers and sold them to a network of coconspirators (Williams, 2002). In 2003 the U.S Secret Service conducted a covert investigation code named “Operation Firewall” to disrupt criminal activity online that was targeting the financial infrastructure of the United States. The investigation, which began in the U.S., quickly became a transnational investigation of a global credit card fraud and online identity theft (Verton, 2004). Underground criminal organizations were identified (Shadowcrew, Carderplanet, and Darkprofits) and charged with operating Web sites whose sole purpose was to traffic counterfeit credit cards, false identification information and documents. The Website provided information on how to commit fraud and sold the stolen information and tools needed to commit the crime (Verton, 2004). IBM predicted in its 2006 Security Outlook report that online threats are becoming increasingly sophisticated. IBM security experts believe that 2006 will see a rise of new and more severe threats (NewsFactor, 2006).

3.1a High Tech Crime Fighting
The technology boom provided state and federal law enforcement agencies with new ways to identify and deter deviant behavior. Law enforcement agencies were given the power and convenience of the Internet to conduct neighborhood surveillances from inside the police station, requiring less manpower and resources, thus saving local governments millions of dollars in training and hourly wages. The ability to use the Internet to share information provided disparate law enforcement agencies with an invaluable tool. The National Crime Information Center (NCIC) provides federal, state, and local law enforcement agencies with a computerized database to track and apprehend suspected criminals. Detectives have the ability to wiretap the information highway to review email traffic, hard drive files, eavesdrop on conversations, and capture emanating electromagnetic radiation. What limits the use of these high-powered technologies from being abused by federal agencies to prevent unlawful search and seizures? Proponents of the 4th amendment raise valid ethical issues surrounding personal privacy and the power of government agencies to circumvent constitutional rights. On the other hand, federal agencies claim that these technological advances help solve and prevent criminal behavior. These issues were debated during a popular court case involving a tech savvy mob boss and the FBI's use of a “top secret” keystroke recording device. The following pages will analyze an article written by author George Anastasia referencing the Nicodemo S. Scarfo case and the ethical issues surrounding the use of highly powered and highly classified technology to convict a common criminal.
When I think about advances in law enforcement technology tools, it is hard not to consider the infamous Big Brother, characterized in George Orwell’s novel 1984. The Big Brother portrayed in this novel tried to instill a sense of fear and paranoia that any type of deviant behavior is subjected to government run surveillance. The government-sponsored surveillance ensured that any behavior characterized as being socially unacceptable would be electronically documented and violators prosecuted in accordance with totalitarian rules. Orwell’s book was written in 1949, but captured a futurological rhetoric on government control and the potential intrusive behavior of government agents in our private lives.

Unbeknownst to Orwell the concept of using technology as a way of controlling behavior, by secretly monitoring and eavesdropping into the personal lives of citizens had become a reality. The various types of surreptitious electronic surveillance and listening devices currently used in law enforcement today are astonishing. The use of the keystroke-recording device as described in the Nicodemo Scarfo conviction is unimaginable for even a computer geek. Incidentally the only concept of the device would be one’s imagination, because the device was highly classified and even 4th amendment discovery guarantees were not provided to the defense lawyers to dispute its validity.

This is what brings us to the ethical and moral issues of using highly classified technological devices to apprehend and prosecute suspected criminals. Government Lawmakers supporting the 4th Amendment to the constitution have gone through great deliberations to ensure that citizens, “will be secure in their persons, houses, papers, and effects, against unreasonable
searches and seizures.” Procedural law requires that law enforcement agencies submit a warrant showing probable cause to validate the intrusiveness of the search. During the preliminary stages, the defense has 4th amendment discovery guarantees to review how the prosecution conducted the search and seizure in an effort to mount a motion to have the evidence obtained thrown out. The federal agents in the Scarfo case circumvented this constitutional guarantee because the keystroke recorder device used to capture the password was labeled top secret and disclosing the evidence to the defense would jeopardize national security. Due to this classification the defense was denied access to the keystroke recorder, to perform its own tests.

The facts of the case were to convict Scarfo on being a bookie and in order to find evidence to support the allegation they needed the password to Scarfo’s computer. The keystroke recorder was used to identify/record the keystrokes when Scarfo signed onto the computer and surreptitiously capture his password. The device was labeled top-secret and negated traditional due process of law. The prosecution exercised its judicial rights under the Classified Information Procedures Act (CIPA), which gives guidance on pretrial deliberation regarding the use and disclosure of sensitive material. Under CIPA the prosecution could not disclose details about how the device was utilized to capture Scarfo’s password.

This article identifies some key issues that government lawmakers will encounter on a more frequent basis. The use of advanced technology to identify and apprehend terrorists are presently in use and the judicial system will be
forced to follow the CIPA guidelines. Lawmakers need to enact laws that govern
the use of classified devices to provide guidance on when highly classified
technologies can be used to obtain incriminating evidence to support the
prosecution case. Clearly, the Scarfo case exceeded the need to use such a
highly classified instrument. Other means of surveillance could have been used
to identify the password without jeopardizing national security.

3.2 Economic Espionage

“Economic Espionage is the greatest threat to our national security since
the Cold War.” Louis Freeh, former FBI Director

Reports from the Defense Investigative Services have identified the Internet as
the fastest growing areas of intelligence gathering by foreign governments and
potential enemies of the United States and allies (ENN Daily News, 2006). American Defense contractors, software producers, and other related industries
have reported unsolicited contact from Eastern European, Middle Eastern and
Far Eastern regions (ENN et. Al). The steady rise of economic espionage
against the U.S. by G-8 countries (Canada, Japan, Britain, France, Germany,
Italy and Russia) is a result of the U.S. investment in research and development,
which is estimated to be $300 billion dollars, more than all G-8 countries
combined (Lexicom Inc, 2003). “Global economic competition has, to a large
extent, replaced the Cold War political and military competition between East and
West. As a result, friends and allies, as well as less friendly countries, now
pursue their national interests through espionage against the United States.
Their goal is to develop a competitive edge in the global market place or boost
military readiness, while drastically reducing their own research and development costs” (Defense Security Service, 2005).

Britain recently deported an Israeli couple for allegedly developing and selling spyware for economic espionage programs (Leyden, 2006). The agents investigating the case accused the Israeli couple of developing and marketing spyware or Trojan horse packages designed to evade corporate firewalls. These programs were sent to three private investigation firms in Israel via emails and infected floppy disks – Modi'in Ezrah, Zvi Krochmal, and Philosof-Balai (Leyden, 2006). The payload of the malware infected the machines and sent stolen documentations to an FTP site and provided other corrupt organizations the ability to take confidential documents from competitors. Each successful installation netted the couple approximately $450.00 (Leyden, 2006).

3.2a Techniques to Mitigate Economic Espionage

The capability to conduct surveillances on LAN and WAN infrastructures has provided corporate network security analyst and law enforcement officials with a mechanism to help deter cyber criminal behavior. Network surveillance provides investigators with a sophisticated crime fighting tool that helps them accomplish the following goals: (a) Confirm or dispel suspicion surrounding an alleged computer security incident, (b) Accumulate additional evidence and information, (c) Identify additional parties involved, (d) Determine a timeline of events occurring on the network, (e) Ensure compliance with a desired activity. There are a number of different types of network monitoring techniques, such as event monitoring, trap-and-trace monitoring, and full-content monitoring.
Event monitoring is based on predetermined rules or thresholds established by the network engineers to monitor specific hardware devices or applications on a LAN or WAN. Events occur when the engineer is alerted that a network monitoring rule or threshold has been acted on and action is required to determine the cause of the incident.

Trap-and-Trace (aka. pen registers) monitoring is a less intrusive way to troubleshoot a network. Also known as a non-content surveillance monitoring type because it summarizes the transaction data by reporting only protocols, IP addresses, and ports. The entire monitoring session does not care about the content of a conversation. This type of network monitoring serves two purposes (1) to protect the privacy of network users (2) to permit system administrators to troubleshoot networks and locate the source of technical problems. The legal requirements for this type of network monitoring are different for law enforcement officers than those rules governing a corporate network security investigator. A law enforcement agent may be required to obtain a court order or subpoena, while a network analyst may not have to. The Electronic Communications Privacy Act (ECPA) under 18 U.S.C 3121 states, “no person may install or use a pen register or a trap and trace device without first obtaining a court order..”, unless one of the three exceptions applies. The first two exceptions allow service providers (organizations) to use trap-and-trace monitors in normal course of their business to ensure proper operation and use; the third exception requires the consent of the user in order to perform a trap-and-trace.
Full-content monitoring is a great tool to detect unlawful or unauthorized activity and establish the identity of the individuals conducting the actions. Full content monitoring yields data that includes the raw packets collected from the wire. Unlike trap-and-trace monitoring, full content monitoring captures the actual communication passed between computers on a network. Additionally, full content monitoring includes packet headers and payloads like pen registers. Law enforcement officials may have to obtain a Title III nonconsensual wiretap. However, the proper system banners and AUP’s afford corporate investigators with the legal remedy to utilize full-content monitoring or perform real-time keystroke capturing.

18 U.S.C. SS2511 is known as the federal wiretap statute. The statute makes it illegal for anyone to intercept wire, oral, or electronic communications while they are being transmitted. This status applies to both law enforcement and non-law enforcement personnel. The only exception to this statute is consent by one of the parties involved in the communication has given prior consent. A corporation can wiretap employees when appropriate policies are in place explaining the right to monitor. Corporations can enforce the right to monitor intruders by having appropriate banners on hardware logins. By forcing an intruder to view the banner and clicking past the warning provides consent to monitor any activity performed on the host network.
3.2b Computer Security Incident Response Team (CSIRT)

The key to successfully responding to a network security attack within any network setting is to develop a response plan that can be executed effectively. The following will provide the goals of a CSIRT team lead during a network/computer security issue. The goals of an investigator responding to a security incident are to help prevent a disjointed or non-cohesive response. The ability for organizations to effectively respond to security incidents will provide a proven method for dealing with security incidents. For example, a Security Incident Response Team (CSIRT) is organized by organizations to respond to security incidents. This team is multidiscipline with the appropriate legal, technical, and other expertise necessary to resolve an incident. Since most CSIRT members have special expertise, and incident response is not required at all times, CSIRT team members are only assembled when an organization requires its capabilities.

The first goal of an investigator is to confirm or dispel whether an incident occurred. The detection of an incident is one of the most important phases during incident responses. Security incidents are normally identified when someone suspects that an unauthorized, unacceptable, or unlawful event has occurred involving an organization’s computer network or data processing equipment. It is important that organizations have a well-documented and simple mechanism for reporting incidents.

The second goal of an investigator is to promote the accumulation of accurate information. This is typically done during the initial response. The data collected
during this phase involves reviewing network-based audit reports and gathering evidence from the following:

- Interviewing system administrators who might have insight into the technical details of an incident.
- Interviewing business unit personnel who might have insight into business events that may provide a context for the incident.
- Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has occurred.
- Reviewing the network topology and access control lists to determine if any avenues of attack can be ruled out.

The third goal of an investigator is to establish controls for proper retrieval and handling of evidence. Most evidence handling procedures are frequently attacked in suppression hearings. To help prevent this from occurring, organizations can appoint evidence custodians and maintain the chain of custody documents. This requires that evidence collected is stored in a tamper-proof manner where unauthorized individuals cannot access it.

The fourth and fifth goal of an investigator is to protect privacy rights established by law and policy as well as allow for criminal or civil actions. An example of this is the 4th Amendment, which protects U.S. citizens from unreasonable search and seizures by the U.S. government. It can be argued that employees have an expectation of privacy on a machine (computer) that an organization owns. To help prevent this from being an issue during an
investigation an acceptable use policy (AUP) can encompass employee’s consent to searching of their computer systems as a standard business practice.

The sixth goal of an investigator is to minimize disruption to business and network operations. Network outage for some organizations can cost millions of dollars in lost revenues. Investigators need to be aware of the cost to the organization if they take a server or host off line for a certain period of time. To help minimize disruptions to business operations investigators should consider investigating incidents during off hours, if possible.

The seventh goal of an investigator is provide accurate reports and useful recommendations to the business. This is an important part in the investigation because investigators will use these reports to refresh their recollection during criminal trials and in training employees about the incident. The challenge for investigators is to create reports that meet the following criteria:

- Accurately describe the details of an incident
- Easy for non-technical decision-makers
- Withstand the barrage of legal scrutiny
- Produced in a timely manner.

Some key points to remember during this phase are to document immediately, write concisely and clearly, and use standard format.

The eighth goal of an investigator is to provide rapid detection and containment. This helps minimize the exposure and compromise of proprietary data. Organizations that are proactive in detecting security incidents take some of the following steps to help an investigator respond effectively:
• Record cryptographic checksums of critical files
• Increase or enable security audit logging
• Build up your host’s defenses
• Back up critical data and store media securely
• Educate users about host-based security.

The ninth goal of an investigator is to protect the organizations reputation and assets. This ties into the response strategy an investigator will use for various types of security incidents.

The tenth goal of an investigator is to educate senior management on the specifics of the security incident. The details of the incident should be high level and depending on the audiences technical back ground should eliminate technical jargons. The information provided will assist the business owners in developing a response to the incident.

The eleventh goal of an investigator is to promote rapid detection or prevention of these incidents in the future. To help investigators accomplish this task they educate users via lessons learned and policy changes. To understand the incident will help prevent reoccurrence in some situations.

3.3 Terrorist Online

“The Internet enables every jihadi to feel part of a larger whole. It enables every angry Muslim to give vent to his or her anger in myriad ways. It enables every Muslim to become a participant in the jihad in his or her own way, with or without a leader. It has strengthened Islamic solidarity. Cyber space has become the spawning ground of jihadi warriors. The use of the Internet by the jihadi terrorists illustrates the folly of dismissing them as irrationals or as persons with a medieval mind. An irrational person or one
with a medieval mind cannot use the Internet as effectively as the jihadi terrorists have been doing." (Raman, 2005)

The previous sections have provided a detailed understanding of how terrorists, hackers and criminal organizations can exploit the genius of the Internet for their own ideological beliefs. Federal investigators have evidence that Islamic terrorists used the Internet covertly and overtly to plan attacks; generate funding, spread propaganda in English, Arabic and various other languages (ADL, 2002). Strong evidence has been uncovered that details how Al Quada sleeper cells operating in the US planned, and effectively executed, the September 11th terrorist attacks. There is concern among industry experts that the Internet itself maybe used as a weapon, to wreak havoc on American critical infrastructures. The US government has discretely voiced concern to the US utility companies that they need to focus on increasing their current network security posture. According to government reports the vulnerability of attacking the US electrical grid has increased. Power companies have increased the efficiency of managing their infrastructure, but by doing so have now opened additional security vulnerabilities in their network. Power companies have transferred control of their generation and control equipment from private internal networks to supervisory control and data acquisition (SCADA) systems that are accessed via the Internet (Blum, 2005)

3.3a Planning and Coordination

It has been proven that terrorists are using the Internet to plan and coordinate attacks against the United States and its Allies. Al-Qaeda sleeper cells used the Internet to plan and coordinate the attacks on September 11th.
Federal officials were able to decrypt thousands of encrypted messages on a computer owned by Abu Zubaydah, an Al Qaeda operative. (ADL, 2002).

To protect their identity the operatives utilized public Internet cafes and communicated using Email accounts that were created using fictional information. By using public libraries or by stealing Internet services from non-secure wireless networks, operatives were able to remain anonymous. The operatives also took advantage of free trials with popular Web-Based Internet services to correspond freely back and forth to other operatives operating outside the US. Information also confiscated from the known operative’s detailed the research and coordination of engaging their targets prior to September 11th. Information provided on the Internet allowed the terror agents to meticulously plan the attack with precision.

3.3b Encryption

Data encryption is the transformation of data into a form that makes it unreadable by anyone without a secret decryption key. Encryption provides the ability to communicate securely between two components without the fear of compromising the information enclosed. For thousands of year’s generals, kings and queens have all benefited with the use of effective and efficient communication to command their army’s and govern their countries. Even then, they all were concerned about their communication plans falling into the hands of their enemies to exploit their secrets and expose their plans of attacks. This concern and paranoia manifested the development of hundreds of codes and
ciphers that were used by kings, queens and military leaders who required confidential communication.

Steganography is the art and science of hiding communication. For example, a steganographic program embeds hidden content in unremarkable cover media in an effort to not arouse an eavesdropper’s suspicion (Provos, 2003). Steganography has been used for years, for example, Roman generals were known to shave off the hair of messengers and tattoo a secret message onto their head. Once the hair grew back the information was hidden until the messenger arrived at his/her location and their hair removed to reveal the message. The key was to know that the person had a tattoo on his head. The alternative solution was to check everyone’s scalp as they passed through the guard checkpoints.

To increase their anonymity on the Internet, terrorists are using un-crackable encryption and stenography to camouflage their planning and coordination secrets. USA today published an article that states, “Osama bin Laden and other Muslim extremist are posting encrypted, or scrambled, photographs and messages on popular Web sites and using them to plan terrorist activities against the United States and its allies. These tactics are so common that these techniques are being taught to Muslim extremist at terrorist camps in Afghanistan and Sudan (Kelly, 2001). The use of un-crackable encryption will allow terrorist networks the ability to communicate without fear of intrusion by law enforcement personnel. FBI Director Louis Freeh testified at a
Senate hearing that “terrorist operatives are thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities”. (Kelly, 2001)

The US National Security Agency (NSA) has been the world leader in encryption and decryption techniques for many years. However, the NSA is now faced with the reality that powerful encryption and decryption techniques are being formulated by Muslim extremist in third world countries, such as Kashmir, Kosovo, Syria, Afghanistan, Yemen, and the Philippines (Kelley, 2001). The technological advances that have provided us with secrecy are now being used against us to conduct clandestine warfare operations on the international information grid. Ahmed Jabril, a spokesman for the militant group Hezbollah in London says, “It’s brilliant”, and “now it’s possible to send a verse from the Koran, and appeal for charity and even a call for jihad and know it will not be seen by anyone hostile to our faith, like the Americans.” (Kelly, 2001).

Terrorists are also using encryption to scramble their phone conversations to prevent interception. The US counter terrorism teams headed by the FBI were actively monitoring Osama Bin Laden’s satellite phone conversations. These eaves dropping actions were somehow revealed and since then all phone calls have been encrypted, thus preventing eaves dropping by US officials.

3.3c Propaganda

After the attacks of September 11th, the US started to reevaluate the freedom and democracy in which we all have become accustomed. Our democratic society that provided us the security and freedom to live was now being used against us by foreign extremists in an effort to deny us the inalienable
right that freedom guarantees. Terrorists are not counting on winning through
military force, their goal is simple: “the goal of terrorism is to fill people with
intense fear, to intimidate people to deliver a political message, and to paralyze
government and commerce.” (Myers, 2001) Our society has succumbed to the
goals of terrorism by creating a plethora of paranoia on when, where and how the
next terrorist attack will occur.

Propaganda is defined as any ideas, facts, or allegations spread
deliberately to further ones cause or to damage an opposing cause. (Merriam-
Webster, 2005). The propaganda strategy currently used by Al-Qaeda is taking
advantage of the anonymity and flexibility of the Internet to further its cause. The
Internet has provided terrorist organizations across the globe with a valuable tool
to solicit for support, sympathy and financial fundraising. The ability for federal
agencies to track and monitor these sites has become a virtually impossible task.
As one site is shut down another web site is brought online with the same
information as the previous one. Terrorist organizations are encouraged to
spread jihad by downloading propaganda to their sites, which is done to ensure
continuity.

The following provides a list of active terrorist propaganda websites:
The wide use of the Internet has provided a global soapbox that provides interested parties with an opportunity to express their global views of conflicts. Websites such as jehad.net is a website created to provide news network Terrorist Orientation Description URL

<table>
<thead>
<tr>
<th>Terrorist Orientation</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spawn of Finsbury Park Mosque</td>
<td>Web site of Abu Hamza Al Masri, under indictment in the US and Yemen for terrorist related activity. Primary purpose of this site appears to be to encourage participation in Islam-inspired violence, aka Jihad.</td>
<td><a href="http://www.shareeah.org/">http://www.shareeah.org/</a></td>
</tr>
<tr>
<td>Hizballah</td>
<td>Site of weekly newspaper, which circulates activities of the Islamic condition in Lebanon and a variety of news articles.</td>
<td><a href="http://www.intiqad.com">www.intiqad.com</a> <a href="http://www.nasrollah.net/">www.nasrollah.net/</a> <a href="http://www.naimkassem.org">www.naimkassem.org</a> <a href="http://www.moqawama.org/">www.moqawama.org/</a></td>
</tr>
<tr>
<td>Hizb ut-Tahrir</td>
<td>An Islamist site that aims its messages to the outside world is that connected to Hizb ut-Tahrir, the Islamic Liberation Party. This site has been banned in Germany for being anti-Semitic and promoting hate and terror</td>
<td><a href="http://www.hizb-ut-tahrir.org">www.hizb-ut-tahrir.org</a></td>
</tr>
<tr>
<td>Palestinian Islamic Jihad</td>
<td>Official site of Palestinian Islamic Jihad/Jihad Islami</td>
<td><a href="http://www.qudsway.net">www.qudsway.net</a></td>
</tr>
<tr>
<td>Kavkaz</td>
<td>Official website of the Chechen jihad</td>
<td><a href="http://www.kavkazcenter.com">www.kavkazcenter.com</a></td>
</tr>
<tr>
<td>Caliphist/Jihadist</td>
<td>East Turkistan, Qaida-allied forces based in Xinjian Province</td>
<td><a href="http://www.et.4t.com/">www.et.4t.com/</a></td>
</tr>
<tr>
<td>Popular Front for the Liberation of Palestine</td>
<td>Official site of Popular Front for the Liberation of Palestine</td>
<td><a href="http://www.kataebabuali.com/">www.kataebabuali.com/</a></td>
</tr>
<tr>
<td>Fatah/Tanzim/Al Aqsa Martyrs Brigade</td>
<td>Official site of the Al Aqsa Martyrs Brigade, the military unit of the Fatah faction of the Palestinian Liberation Organization</td>
<td><a href="http://www.fatehfighters.org/">www.fatehfighters.org/</a> <a href="http://www.palvoice.com/forums/index.php">www.palvoice.com/forums/index.php</a></td>
</tr>
</tbody>
</table>
It is hard to peruse the Internet without being a victim of deception. Stealth Internet Protocol Technology conceals or cloaks the user's computer identity from being seen across the Internet or network, while it allows the user to freely surf the Internet or network safely. Since the user cannot be identified or located, the user's risks are greatly reduced from any threats of scans, probes or attacks.

4.0 Lessons Learned

As presented in this research paper we have learned how to use deception as a tool to achieve certain goals and objectives. Our understanding of deceptive tactics can be traced back to nature, biblical scriptures, the Internet and technological advances of stealth technology. We have become a society that has to some extent evolved as a result of our pursuance and prevention of deceptive tactics. I have mentioned in this paper that with every innovated idea there is always a mechanism that tries to destroy the integrity of the original design. Technology has become a determinant force that seems to drive change, both negative and positive.

Online criminals and terrorist organization have used the globalization of the Internet to expand their iniquitous beliefs. Research has proven that the technological advances of computers have provided international criminals and terrorist cells with an effective tool that exploits the inexperience and untechnical knowledge of online computer users.

My research on deceptive tactic has provided information about domestic and foreign corporations that use deceptive marketing techniques to capture what Web sites are most frequently viewed by loading spyware programs onto
computers. These same corporations are investing millions of dollars to secure their intellectual properties against industrial espionage, hackers and other malicious code.

Research has shown that the use of deception on the global information grid by Criminals, Terrorists and law enforcement agencies has been a catalyst for technological advances within our society. As technological advances have increased to protect against online crime and trickery so have the knowledge of how to deter these types of tactics.

We have become a society who has become very dependent on technology to continue our way of life. We depend on technology to send and receive written correspondence, manage our finances, and maintain the daily production lines for food, drugs, automobiles, and utilities. The fear among those whose job is to ensure this way of life is sustained is that the Internet will become the next full scale terrorist attack. Whether the Internet will provide the means to command and control the events or deliver the code to complete the weapons system, the Internet has become a Web of Deception.

In closing, I wanted to provide this paper to help online users understand the complexity of crime and terrorism on the Internet. Additionally the paper provides a in depth understanding about the various type of deceptive tactics that users may encounter when using the global information grid. I enjoyed writing this paper and sharing an information about one of the worlds greatest invention.
5 References


