Information Warfare

Brandon Himes
bchim11@sru.edu

Patricia A. Joseph
patricia.joseph@sru.edu
Computer Science Department
Slippery Rock University
Slippery Rock, PA 16057, USA

Abstract

Information warfare is the use of information as an instrument of war. Information warfare is a relatively new topic. The development of new technologies such as broadband Internet access, wireless networking, and the dependence of governments and businesses on the functionality of the Internet has been a catalyst for information warfare. Information warfare can take many forms. Some are purely destructive such as Distributed Denial of Service (DDoS) attacks and the creation of viruses, but other methods of information warfare resemble normal use of the Internet such as organizing groups and disseminating information. Although information warfare is typically destructive and is mostly used for terrorism or crime, it can also be used as a powerful, constructive tool that empowers law enforcement and grassroots movements.

Keywords: leading edge technologies, networks, security

Introduction

Information warfare is the use of information as an instrument of war. Information warfare is a relatively new topic. The development of new technologies such as broadband Internet access, wireless networking, and the dependence of governments and businesses on the functionality of the Internet has been a catalyst for information warfare. Information warfare can take many forms. Some are purely destructive such as Distributed Denial of Service (DDoS) attacks and the creation of viruses, but other methods of information warfare resemble normal use of the Internet such as organizing groups and disseminating information. Although information warfare is typically destructive and is mostly used for terrorism or crime, it can also be used as a powerful, constructive tool that empowers law enforcement and grassroots movements.

Methods of Information Warfare

A first destructive method of information warfare is called "Google bombing." A Google bomb is a tactic used to alter the search results of the Internet's most prolific search engine, Google. A Google bomb is created by Internet users--often bloggers or message board users--posting links to the web site of their victim and titling their link with the desired search phrase they would like that page to appear on. When Google crawls the web to generate its search results, each instance of the aforementioned hyperlink raises the rank of the victim's page on Google's search results. In order to ensure that the victim's web site will be the first result on Google, there must a large quantity of hyperlinks. This is why blogs and message boards are often utilized. Users update information that appears on every page of their blog or on every post on a message board. This is an effective way to propagate the number of hyperlinks.

Although this tactic may not seem inherently destructive, it becomes so in the way it is typically used. Often the search terms are ad hominem attacks or slanderous speech against the victim of the Google bomb. One specific example of this is the G. W. Bush Google bomb. Due to the multitude of links posted to the White House's online biography of George W. Bush that are titled "failure," the search results for that keyword bear a link to the biography as the first result. Google has repeatedly defended the exploitation of its search results as an accurate representation of how other sites feel that a site should be categorized ("'Miserable Failure' Links to Bush," 2005). This method of information warfare is not inherently destructive. However, exploiting Google's search results has little application other than to make disparaging references making it one of the ways that information warfare is used to destructive ends.

A second destructive method of information warfare is Distributed Denial of Service (DDoS) attacks. A DDoS attack is a variation of a Denial of Service (DoS) attack. A DOS attack is when a user repeatedly requests data from a server in order to tie up all of the server's resources until it is so overworked that it grinds to a halt. A DDoS attack is only different from a DoS attack in that it is a distributed attack. This means that many users simultaneously use up resources, making the attack much more effective (Acohido, 2005). One instance of a DDoS attack being used for information warfare was during post war period in Iraq, a DDoS attack was used to disable the Al Jazeera English language web site by regime sympathizers ("'Miserable Failure' Links to Bush," 2005). Just as the majority of information warfare tactics are destructive, a DDoS attack is purely destructive.

A third type of information warfare that is potentially very destructive is attacks on industrial control systems. Since many industrial control systems such as the electrical power, water, telephone and television systems are now run by computers that can be controlled remotely via the Internet (Dougherty, 2005), this means that these systems are vulnerable to attack from the Internet. Such an attack was thought to have taken place during the blackout that left parts of Canada and the eastern United States without power. Though after a thorough investigation by the FBI it was found that the blackout was in fact not caused by an attack but by a failure in the system itself. This does not discount the fear that such an attack could take place. After the conclusion of the FBI investigation, the report warned that such an attack is a possibility that we must defend against with vigilance ("FBI Concerned about Threat of Terror-Induced Blackouts," 2005). Attacks on industrial control systems present a real danger to the population they service and represent the most dangerous of the threats of information warfare.

A fourth threat posed by information warfare is the threat of highly trained mercenaries capable of launching an arsenal of information warfare attacks. Though even an amateur attacker can cause damage using information warfare and only basic techniques, the greater threat is from those trained and experienced in using information warfare to cause damage. The prospect of information warfare mercenaries is very real and there are documented cases both domestically and abroad. One such case is that of Jay R. Echouafni, who was investigated by the FBI and was found to have hired a mercenary to use a variety of information warfare attack against his business competitors (Bryan-Low, 2004). Yet another, more frightening, example of information warfare mercenaries being used en masse is that of North Korea. South Korea, concerned about the potential of an information warfare attack, investigated reports that North Korea had established a school for the training of information warriors (MacKinnon, 2005).

The findings of this investigation were surprising given the relatively low amount of cutting edge technology in North Korea. South Korea's investigation found that North Korea had established an "Automated Warfare Institute" and that it trained 100 highly specialized information warriors a year (MacKinnon, 2005). The threat of a highly trained army of information warriors is one of the grimmest threats that information warfare poses. The fact that this army is trained in North Korea expresses the true threat that information warfare poses. North Korea does not supply its own Internet access, have very advanced technology, or even have reliable electrical grids, yet it is

capable of producing information warriors. What can be expected of more advanced countries who take initiative to participate in information warfare? Though an army of information warriors trained to defend could possibly have constructive application, the only instances of trained information warriors have been used for purely destructive purposes, posing a great threat to their adversaries.

A fifth threat of information warfare is the creation of viruses. Viruses are malicious code written expressly for the purpose of penetrating security and causing damage. Viruses are the oldest form of information warfare and therefore are the threat that the general population is most equipped to deal with. There are many companies that produce anti-virus software that is used to defend users against such attacks. Some examples are Norton, McAfee and others. Despite this, viruses cannot be completely defended against and as a consequence they often cause large amounts of damage.

Some of the most destructive viruses ever devised are Sasser (2004), Blaster (2003), and Nimda (2001) which caused 3.5 billion, 1.5 billion, and 1.5 billion dollars worth of damage, respectively (Vogelstein, 2004). Viruses are probably the most common type of attack used in information warfare. It is common for viruses to be used only for the purpose of terrorism. They are seldom used on one group or another, but rather are released on the general population to cause damage. Microsoft, whose products are the target of many viruses, often has offered a reward for any information leading to the author of the virus being brought to justice. This is seldom effective because frequently viruses are launched from geographic areas where the United States holds no authority. Viruses are certainly a destructive and threatening means of information warfare.

A sixth type of information warfare, and perhaps the most serving to the warrior's cause, is hacktivism. Hacktivism is a compound of "hacking" and "activism". Hacktivism utilizes many other means of information warfare but tends to center more on web sites as the goal of hacktivism is to be as public as possible in order to influence the feelings and opinions of others. Hacktivists often uncover passwords or manipulate web servers in order to deface the website of their victim in order to put their message into the public eye. Hacktivism also includes other means by which to convey the message of the hacktivist's ideology.

Information Warfare Activities

One recent example of hacktivism took place in Italy. The Italian legislature made a decision that many homosexuals felt infringed on their rights. Hacktivist sympathizers attacked the Italian government by planting a backdoor Trojan virus into the government's computer network (Sturgeon, 2005). A "backdoor Trojan virus" works by putting seemingly innocuous code onto a machine then once the code is inside the code changes to become malicious. A "backdoor" virus is one that, once inside a system opens a security hole that allows a remote user to perform a multitude of actions on the user's machine without the user's consent. The Italian hacktivists used this backdoor to cause homosexual pornography to play on the screens of all of the computers on the Italian government's computers (Sturgeon, 2005). Although hacktivism can certainly be used to destructive ends, it is not nearly as costly as other means of information warfare and is seldom used for terrorist ends.

Unlike the preceding types of information warfare a seventh type of information warfare, using the Internet to organize and communicate with supporters is almost always a constructive act. The Internet enables large, geographically dispersed groups to organize, plan and coordinate their efforts to achieve the group's goals. This is one of the reasons that the Internet was created. While its peacetime applications were originally envisioned at its creation, the Internet has many applications in communication and administration in wartime.

A group that uses the Internet to coordinate their side of a conflict is the Zapatista movement in Mexico. The Zapatistas are a group of indigenous people of Chiapas, Mexico. They have been in a long and violent conflict with the Mexican government over a dispute about the ownership of their land. The Mexican government has attempted many times to forcefully remove the Zapatistas from the land in question with little to no success due to the heavy military resis-

tance of the men, women and children of the Zapatista (Accion Zapatista de Austin, 2005). However, realizing that time was on the side of the Mexican government, the Zapatista decided that they would need a better consolidated force and the opinion of the world on their side if they were to win the conflict. In order to do this the Zapatista moved their organization into cyberspace. The Zapatista web site helps convey information and organize the movements of the Zapatista while also telling the world of their righteous struggle to keep their ancestor's lands (Accion Zapatista de Austin, 2005). This method of information warfare is not destructive to the enemy, unlike those that preceded it, but it is constructive and positive in any light.

Computer Network Security

Closely related to organizing support and another means of information warfare that is constructive is basic communication. This method of information warfare is the essence of the Internet. What is the Internet if not a means of communicating information?

Communication, when considered in the context of war, is a means of information warfare. Often a military action will attempt to isolate an area, preventing it from communicating from the rest of the world. Information warfare then becomes essentially communication.

During the days after the United States invasion of Iraq all means of communication in Baghdad were destroyed. This left many families, friends, and loved ones to wonder what had become of the people of Baghdad. In the days following the invasion, recognizing the need to communicate, a few Iraqi entrepreneurs invested in a mobile satellite Internet receiver. Along with a store front and the necessary computers, this became Baghdad's only Internet café. Iraqi citizens now use this café to broadcast the conditions of Baghdad's condition as well as to contact their family members to let them know that they are safe ("In Baghdad, Rebuilding the Net," 2005). Connecting the Iraqi people with the outside world and to their families would not have been possible without this constructive means of information warfare.

A third constructive means of information warfare is the identification of potential terrorists and criminals. National security has become an all important task. Since the September 11th attacks, the U.S. government has been seeking means of ensuring that it is safe from terrorist plots. One method of achieving this goal is to use information warfare to seek out and identify those that would commit acts of terror. This can be done by comparing information that has been collected by national agencies. Comparing such data as flight records, citizenship status, lists of known criminals and background checks software applications can find commonalities that may have gone unnoticed.

One such piece of software that is used to identify potential terrorists is Matrix, an application that pulls data from many databases. The power of Matrix was most strikingly displayed when it identified common ties between all of the September 11th highjackers after the fact. Matrix is now used in many airports to identify individuals that may pose a threat to security ("LexisNexis buys counterterror software maker," 2005). Another means of distributing information to help identify terrorists and aid in law enforcement is the National Homeland Security Network. This network allows many of the U.S. government's agencies such as the Department of Homeland Security, the Federal Bureau of Investigation and the Central Intelligence Agency to share information they have gathered in order to prevent terrorist attacks (Swartz, 2004). The prevention of terror that this means of information warfare provides is not only constructive but actually prevents destructive means of physical warfare.

Yet another means of information warfare is the electronic verification of documents. Counterfeit documents present an immense problem for those that rely on the use of physical documents for verifying identity. Despite advances in the technology used to produce identification documents, counterfeiting technology has managed to adapt and change its methods. Electronic verification of documents presents an impasse for counterfeiters. A copy of the original document is obtained electronically and displayed to verify documents authenticity. Counter-

feit documents can be easily recognized and confiscated.

The most effective instance of electronic document verification has been developed and is now used in American airports. As a foreign visitor enters an airport in the United States, the identification documents they provide are electronically verified. A picture of the electronic document is displayed for airport personnel to verify the authenticity of the documents. This verification process allows airport authorities to inspect identification documents for counterfeiting such as altered photographs and inconsistent information. Preventing those with counterfeit identification documents helps to keep out terrorists and other threats to national security (Mangaliman, 2005). The electronic verification of documents is certainly a positive use of information warfare that protects the masses from those who would use them to aid terror and crime.

A final means of information warfare is electronic law enforcement. Through the use of information warfare electronic sting operations can be performed by law enforcement agencies. The ability to perform such covert operations allows local and federal law enforcement agencies to catch criminals whose crimes might otherwise be beyond the scope of law enforcement officials.

The most important use of information warfare to apprehend electronic criminals in the United States was Operation Web Snare. During the course of Operation Web Snare federal law enforcement agencies placed decoy targets that were sure to attract electronic criminals in cyberspace. As attacks on the targets were made, law enforcement officials tracked down the attackers and brought charges against them. Several hundred electronic criminals were charged for their crimes who would otherwise have continued to commit crimes unbeknownst to law enforcement (O'Rourke, 2004). Operation Web Snare displayed the positive use of information warfare as a tool to apprehend electronic criminals.

Conclusions

As with so many other issues that involve new technologies and change, information warfare has proven to have two sides to its coin. The threat of viruses proves to be costly economically. DDoS attacks also stand to prevent the technology that world depends on in its daily live to be disrupted which is at times a monumental inconvenience. Far greater a threat than either of these negative uses of information technology is the prospect of an attack on an industrial control system which could not only inconvenience the masses but cause the loss of vital resources needed to live such as electricity and water.

Yet along with such negative uses, information warfare also offers many positive outcomes. One such outcome is the organization of grassroots movements which need to harness the power of information warfare to level the playing field against their colossal foes. Another positive is the ability to communicate no matter what the conditions, which is very valuable. Perhaps the most valuable positive of information technology is to protect the world from those that would do it harm by means either electronically or otherwise through the use of information warfare as a law enforcement tool. Despite the typically destructive nature of information warfare through methods such as DDoS attacks, Viruses and attacks on industrial control systems, the use of information warfare for positive purposes such as the organization of grassroots movements, communication during wartime and law enforcement confirms information warfare's status as a tool that can be used for positive as well as destructive ends.

References

Accion Zapatista de Austin (2005) "Neoliberalism: Zapatismo in Cyberspace," *Zapatismo*, March 2005, Available at http://studentorgs.utexas.edu/nave/cyber.html

Acohido, B. (2005) "Hacktivists Protest War by Attacking Web Sites," *USA TODAY*, March 2005, Available at http://www.usatoday.com/money/world/iraq/2003-03-25-hacktivism_x.htm

Bryan-Low, C. (2004) "Growing Number of Hackers Attack Web Sites for Cash," *Wall Street Journal*, 30 November 2004, p. A1, 2004.

Dougherty, J. (2005) "Report warned power vulnerable to terror," *WorldNetDaily.com,* March 2005, Available at http://www.wnd.com/news/article.asp?ARTICLE_ID=34212

"FBI Concerned about Threat of Terror-Induced Blackouts" (2005) *CNN News,* March 2005, Available at http://www.cnn.com/2003/ALLPOLITICS/09/04/blackout.hearing/

"In Baghdad, Rebuilding the Net" (2005) *USA Today*, March 2005, Available at http://www.usatoday.com/tech/world/2003-05-23-baghdad-online_x.htm

"LexisNexis buys Counterterror Software Maker" (2005) *Sun-Sentinel*, March 2005, Available at http://search.ep.com/login.aspx?direct=true&db=nfh&an=2w6335931

MacKinnon, R. (2005) "Hermit Hackers," *Foreign Policy*, March 2005, Available at http://search.epnet.com/login.aspx?direct=true&db=aph&an=8800024323

Mangaliman, J. (2005) "INS' Ziglar Unveils New Airport Security Computers that Track Foreign Visitors," *San Jose Mercury News*, March 2005, Available at http://search.epnet.com/login.aspz?direct=true&db=ngh&an=2w7084115

"'Miserable Failure' Links to Bush" (2005) *BBC NEWS*, March 2005, Available at http://news.bbc.co.uk/2/hi/americas/3298443.stm

O'Rourke, M. (2004) "Operation Web Snare," *Risk Management*, November 2004, Vol. 51, Issue 11, p. 8, 2004.

Sturgeon, W. (2005) "Gay Porn Hackers Strike Italian Politics," *Silicon.com*, March 2005, Available at http://software.silicon.com/malware/0,3800003100,39126103,00.htm

Swartz, N. (2004) "U.S. Anti-Terrorism Network Enables Data Sharing," *Information Management Journal*, June 2004, Vol. 38, Issue 3, p. 12, 2004.

Vogelstein, F. (2004) "Why Hackers Are a Giant Threat to Microsoft's Future," *Fortune*, Issue 8, p. 263, 2004.