

FHSMUN 31
UNITED NATIONS OFFICE ON DRUGS AND CRIME

COMBATING DIGITAL CRIME

Introduction

With the worldwide proliferation of the Internet, countries face a new and constantly changing problem in Internet-related crime. The ramifications and difficulties in combating Internet-related crime are much more nuanced than they may appear at first blush. The problem extends well past the lighter examples such as the American recording industry's battle against pirated music or Twitter's battle with Iranian cyber-terrorists. Rather, as the world transitions to an increasingly digital model that sees larger amounts of sensitive information, intelligence and national and international communication utilizing the Internet, security becomes an integral issue.

Cyber Crime

Internet-related crime is a very contemporary issue; the Internet has only started to become widely accessible in the last fifteen years. As a result of this, the international response has been much slower as it is oftentimes difficult to even fully define the problem, let alone articulate laws to combat it. For the sake of avoiding unnecessary semantics within the United Nations Office on Drugs and Crime (UNODC), the body will attempt to categorize digital crime into three categories: crimes that target computer networks or devices directly for personal gain (Cyber Crime); crimes facilitated by computers or networks, targeting a third party that is independent of the device or network (Cyber Terrorism). A third category of Internet-related crime does exist but focuses on the exploitation of children through pornography and child grooming (sexual solicitation of children by adults). Though serious, this last category falls more under the jurisdiction of other UN bodies and is being addressed independently of the UNODC.

Cyber Crime, for UNODC purposes, will refer to examples of crimes that primarily target networks or devices in and of themselves. These crimes typically tend to be less destructive than acts of cyber terrorism as they usually target just one, or a small group of individuals via a single computer or network, thus victimizing only those using the affected computer or network.

While Cyber Crime is not to be taken lightly, it is decidedly less dangerous than its counterpart, Cyber terrorism. Typically, the aim of Cyber Crime is little more than small personal gain, the crimes tend to victimize individuals rather than governments or nations and in a way Cyber Crime may be harder to keep tabs on and stop than Cyber terrorism as a result of its smaller, less ambitious nature and the ease with which cyber criminals may operate.

Examples of Cyber Crime would include: malware; computer viruses; denial of service attacks; fraud and identity theft; and phishing scams. Malware is short for

malicious software and is designed to infiltrate a computer system without the informed consent of that system's owner. The terminology is used to refer to a variety of forms of the aforementioned software such as viruses, worms, Trojan horses, spyware, dishonest adware and crimeware. Malware is the element that typically enables all other forms of cyber crime as it is what physically attacks the computer itself and enables further crimes to be committed.

Crimeware is software that is designed to specifically automate cyber crime. This form of malware perpetrates identity theft in order to access a computer user's online financial services accounts and payment information from online retailers for the purpose of taking funds from those accounts or completing unauthorized transactions that benefit the programmer controlling the crimeware.

Viruses, worms and Trojan horses are actually fairly similar in their aims though their methods differ. Virus is a term oftentimes erroneously given to all malware-related computer issues, but a true virus has no reproductive ability and must be spread from one computer to another via some form of executable code. A virus needs a host, typically some type of file or directory and in order to be spread that file or directory needs to be carried over to the target computer via a floppy disk, CD, DVD, USB drive or (as has become more problematic recently) it can now be sent over the Internet. Viruses almost always cause some form of damage, though sometimes it is negligible if noticeable at all; typically it is limited to just the corrupting or modifying of files, programs or directories on a given computer.

A worm acts in much the same way as a virus, only it needs no host file. Rather, a worm is a self-replicating program that uses a network to send copies of itself to other computers on that network without any intervention. Worms almost always cause some sort of harm to the network, even if just by consuming bandwidth. A Trojan horse is a non-self-replicating malware that appears to perform a desirable function for the computer user but instead offers unauthorized access to the user's computer system.

The many forms of aforementioned malware, as well as many undefined (in this guide), examples are the tools through which other cyber crime can be committed, acts such as identity theft, fraud, phishing scams and denial of service attacks. As has been previously stated, crimeware, Trojan horses and other malicious software can be used to steal identities, gain access to financial resources and commit various acts of fraud. Likewise, phishing is used to much the same end as crimeware and Trojan horses, but rather than taking the form of malware it takes the form of a website, email or in some cases instant message that resemble the look and feel of an established business or institution but serve only to steal an individual's information, passwords or credit card information when entered.

While these attacks may victimize one individual or several across a network, the ramifications of these acts can be much further reaching. Fraudulent transactions have effects on not only the victims of the identity theft but also presents issues for banks and

businesses and serves to drain resources from government and police bodies that must then investigate (typically without much success) the crimes.

Another form of Cyber Crime is a Denial of Service attack. As of this point in time, Denial of Service (DoS) attacks still constitute cyber crime rather than cyber terrorism but the distinction is becoming increasingly less defined. A DoS attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

The most recent example of such an act was the December 2009 hacking of the Internet site Twitter by a self-proclaimed group of Iranian terrorists. The attack was especially pertinent as a result of Twitter's influence during the conflict over the Iranian elections in June 2009, but the aims and intentions of the group attacking the site arguably fell more in line with terrorist objectives than with those of a cyber criminal. While DoS attacks have traditionally fallen in line more with the objectives of cyber criminals in the past, it is worth noting that as the world transitions to a more internet-reliant model such attacks also serve terrorist interests by undermining integral government servers and making necessary services that had been made available through the internet inaccessible to large portions of a country's population. As of now, DoS attacks straddle the line between acts of cyber crime and acts of cyber terrorism.

Digital Piracy/Copyright Infringement

There are other examples of cyber crime as well, though in these instances the international repercussions may be less than the issues posed to individual countries, for instance, copyright infringement. In a way, copyright infringement serves as a microcosm for the entire issue of cyber crime. The parties victimized by copyright infringement are typically individuals and businesses, mostly authors, musicians and those associated with television and motion pictures. Despite international copyright laws, however, the parties responsible for the dissemination of copyrighted materials are often located in countries without strict laws and restrictions on Internet activities. Countries in Eastern Europe and former Soviet states are some of the biggest digital offenders, serving as a safe haven for hackers and those partaking in digital crime.

The issue of digital piracy of copyrighted materials is a fairly divisive one. Groups like the Recording Industry Association of America (RIAA) as well as various watch-dog organizations and artistic groups in mostly Western nations tend to paint the issue as one of the more grievous crimes being committed across the internet. But despite the somewhat disruptive ramifications and the economic damage it does, a good portion of the world feels that the problem is not large enough to merit exceedingly large international attention.

The problem is two-fold: the victimized parties tend to be a fairly wealthy subset of people in Western countries and the means through which copyrighted materials are

circulated are not always clearly understood, clearly illegal or in a position to be well-legislated or regulated. For instance, the BitTorrent (oftentimes referred to simply as a torrent, BitTorrent also refers to a specific torrent client as well) is a commonly used Peer to Peer (P2P) method of downloading files and information and is commonly used to pass along copyrighted materials. The bitTorrent is one of the most common protocols for transferring large files, and it has been estimated that it accounts for approximately 27-55% of all Internet traffic (depending on geographical location) as of February 2009. The issue with torrent files, however, is that they do not contain the actual copyright information but rather serve more as a map or instruction manual for downloading smaller bits of the file from other individuals and then reconstructing said file on the machine.

The BitTorrent protocol allows users to disseminate only a piece of a file in conjunction with other users that have other complementary pieces. The result is that individuals can download files rapidly without drastically reducing bandwidth. One of the other side effects is that as a result of the incomplete pieces of copyright material being sent, it is difficult to prosecute for copyright infringement. Whereas older P2P servers and other methods saw a more singular transfer where one individual computer was sending one file to another computer, these transfers occur across numerous machines and networks. The question of whether individual pieces of a copyrighted file still bear the same restrictions as whole copyrighted files has been an issue in addition to the fact that the torrent file itself is not, in and of itself, a violation of copyright laws but rather a set of directions for a computer on how to break the law. In addition, the technology is also used for legal activities as well. As such, making the protocol illegal (as some have suggested) would be highly impractical in addition to infringing on the rights of individuals who utilize the technology for just purposes.

In addition to the technical issues, there are problems with the locations of copyright violators. Many offending parties are located in states where laws regulating the use of the internet are either years behind more developed nations or even purposely set up in a way to allow for such activities. As mentioned above, countries in Eastern Europe, former Soviet states and an increasing number of Middle Eastern states are seeing a spike in illegal activity on the internet, not just limited to copyright infringement.

For the purposes of the UNODC, the committee will focus on only certain issues with regard to copyright infringement. The committee will focus on conditions that foster the practice (in addition to other illegal internet activities) but the practice itself is outside the scope of the UNODC and may be left to individual governments and other agencies to police. Rather, the UNODC is interested in other forms of Digital Crime that endanger a greater portion of the international community, not the pockets of a select group of wealthy artists.

Digital Drug Trafficking

Drug traffickers are increasingly taking advantage of the Internet to sell illegal substances through encrypted e-mail and other Internet Technology. Some drug

traffickers arrange deals at Internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in Internet drug trades could also be attributed to the newfound ability to eliminate face-to-face communication. These virtual exchanges exude a safer environment for the transactions that may entice otherwise disinclined individuals to more comfortably purchase illegal drugs. The more criminal effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. Furthermore, drug recipes (such as those meant for making methamphetamines and other similar chemical drugs) were carefully kept secrets. But with modern computer technology, this information is now being made available to anyone with computer access.

Cyber Terrorism

Cyber terrorism is a distinction given to acts that utilize a computer or network to attack a third party. There are known examples of cyber terrorism, but much like with cyber crime and all forms of digital crime as the internet evolves, the methods and creativity of digital crime continues to evolve with it. The definition of cyber terrorism as given by Kevin G. Coleman of the Technolytics Institute is “the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.”

Coleman’s definition fits in with the UNODC-proposed categorization of cyber terrorism, acts such as the previously mentioned attack on Twitter by Iranian cyber-terrorists are meant more to undermine a site and cause general panic than to cause any sort of actual damage (besides a negligible hit to ad revenues) but acts of cyber-terrorism targeting larger more integral servers and computers could potentially yield nightmarish results.

Currently, the UN response to Cyber Terrorism has been lacking and any response from the international community has been mostly limited to Western countries. The Secretary of State for the United States, Hillary Clinton, recently called upon the North Atlantic Treaty Organization (NATO) to formalize a plan to combat cyber-terrorism, but much like the rest of the international response, the member states of NATO lack regional influence to combat digital crime at its site. In order to fully engage the issue, the entire international community must come together, as unlike many other issues that face the world, even the smallest of countries can have a major role in regard to Internet-related crime.

Examples of Cyber-Terrorism

One of the biggest issues in the battle against digital crime, specifically with regard to Cyber Terrorism, is the lack of documented methodology in performing a digital attack. As a result, portions of the international community and proponents of less

stringent internet restrictions have made the claim that cyber terrorism is more an issue of hype than of legitimate threat. While this opinion has not been widely adopted by the international community, it does still serve to undermine the issue in much the same way as the dissenting opinion on man-made environmental change manages to muddy that debate.

Recent examples of Cyber Terror are numerous, though the ramifications of each act range in terms of degree of severity. Over a decade ago in 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Also in 1998, one of the first successful Cyber attacks was performed when Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the Internet Service Provider's (ISP) users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the Webs site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

In 1999, an act of cyber terror occurred against NATO computers. The computers were flooded with email and hit with a denial of service (DoS) attack. The hackers were protesting against the NATO bombings in Kosovo. Businesses, public organizations and academic institutions were bombarded with highly politicized emails containing viruses from other European countries.

2000 saw the first documented use of malware as several worms were released that took advantage of holes in Microsoft operating systems, though the first truly dangerous worms failed to materialize until 2003 when a worm called the Slammer (a.k.a. Sapphire) worm infected thousands of consoles in about 30 minutes across numerous countries including the US, the Republic of Korea, Finland and Japan. The worm managed to affect numerous networks including airlines and banks and even disabled a security monitoring system at a nuclear power plant in Ohio.

2001 saw an Australian man gain remote access to sewage systems in Maroochy Shire and dump thousands of gallons of sewage into the local waterways. At about the same time, terrorists in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. Fortunately, however, the culprits were stopped before damage actually occurred.

More recently, there has been a spike in cyber-crime as each day thousands of people gain access to the internet. The Russian Business Network (RBN) was registered as an Internet site in 2006. Initially, much of its activity was legitimate. But the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad". It offers web hosting services and Internet access to all kinds of criminal and objectionable activities, with individual activities earning up to \$150 million USD in one year. It specialized in and in some cases monopolized personal identity theft for resale.

In 2007, Estonia saw one of the strangest examples of a cyber terror attack when an unknown group perpetrated a massive cyber attack in response to the removal of a World War II monument from the city of Tallinn. The attack took the form of a DoS in which selected sites were bombarded with traffic in order to force them offline; nearly all Estonian government ministry networks as well as two major Estonian bank networks were knocked offline. In addition, the political party website of Estonia's current Prime Minister Andrus Ansip featured a counterfeit letter of apology from Ansip for removing the memorial statue. While a single man was convicted of launching the attacks in 2008, the initial belief from Estonia was that it had been perpetrated by Russia, meaning this attack actually served to destabilize the relationship between two states, a far graver consequence than the denial of service on numerous Estonian government websites.

In November 2007, another former Soviet state was victimized by cyber criminals when the website of Ukrainian president Viktor Yushchenko was attacked by a radical Russian nationalist group, the Eurasian Youth Movement. Though many of these attacks seem superficially unimportant or lacking grave consequences, they also demonstrate a propensity for much greater damage. Whether it's disabling a country's financial systems, stealing vital intelligence or destabilizing diplomatic relationships in a region, cyber terrorism bears a very real and threatening prospect in the future and one that must be addressed.

Quantifying the Risk of a Cyber Attack

To understand the potential threat of cyber terrorism, two factors must be considered: first, whether there are targets that are vulnerable to attack that could lead to violence or severe harm; and second, whether there are actors with the capability and motivation to carry them out. While a great number of nations employ very advanced digital security, the ability to attack vital computer systems is evolving as fast, if not faster, than the corresponding security measures. The United States, who many consider to be at the forefront of digital security, has been victimized a number of times by cyber attacks on their intelligence servers. Countries like China, Greece, India, Israel, and the Republic of Korea have all been in the spotlight before by the US media for attacks on information systems related to the CIA and NSA. Though these attacks are usually the result of curious young computer programmers, the United States has more than legitimate concerns about national security when such critical information systems fall under attack. In the past five years, the United States has taken a larger interest in protecting its critical information systems. It has issued contracts for high-level research

in electronic security to countries such as Greece and Israel to help protect against more serious and dangerous attacks.

While even the most proactive of states are at a digital security risk, lesser developed countries choosing to utilize the Internet for sensitive national functions find themselves situated in very precarious territory. And as states continue to transition into a web-model that sees even more of their integral services as well as good portions of their country's private commerce come online, the areas of vulnerability that can be exploited by cyber criminals continue to grow.

The second of the two factors in assessing the risk of a cyber attack is the capability and motives of the perpetrators. As has been evidenced by numerous examples and advancements in computer-related technology, the capability to stage digital attacks increases on a daily basis, as do many of the motives (as fueled by regional and international conflict). A distinction has to be made among the three basic types of cyber terrorists. The professionals, those who, by order of their sponsors, aim at inflicting physical or cyber damage onto victim's resources, the amateurs, who find pleasure in applying cyber graffiti defacing corporate or government websites, and the thieves, who have immediate personal economic benefit from their actions.

The professionals are cyber terrorists who operate behind a variety of façades – political extremists, religious fanatics, revolutionaries, and the like. The fact remains that cyberspace allows the cyber terrorists anonymity, and the potential impact of their attacks, as well as their timing, is unpredictable. It must be recognized that the technical education, the experience and the expertise of the cyber terrorists, especially of the professionals, parallels that of the networks design experts. In addition to this technical background, cyber terrorists also develop knowledge on the network architecture of the victim's resources. It must also be recognized that professionals are not malevolent volunteers, but well sponsored operatives of political, military, or economic interests, either state or private.

Problems Combating the Issues

Currently the biggest issue facing the international community in the battle against digital crime, specifically in regards to Cyber Terrorism, is the fragmented legal front put forth by the rest of the world. There exists no universal set of laws or regulations for the Internet, rather it is up to each individual state to establish its own laws and police the internet as it deems fit.

This results in a broad range of regulation spanning from nearly non-existent laws and regulations in some countries to nearly fascist regulations in other. For instance many of the states in the former Soviet bloc have next to no law policing the Internet. The result of this lack of consistent regulation is that a number of illicit and highly illegal digital crimes are perpetrated within their borders against the rest of the world on a daily basis. Conversely, China has some of the strictest Internet regulations in the entire world. Chinese citizens have access to a very subjugated version of the Internet where

information is heavily controlled and activity is highly monitored. Even the perception of wrongdoing on the Internet in China can lead to incarceration and social sites such as Facebook are completely illegal.

One of the biggest problems facing the defense of digital crime is the disparity in perception by many of the countries around the world. While larger more developed countries may view these crimes as a matter of national defense and a major international issue, other countries choose to prioritize development issues or other security issues above digital security. By some legal definitions, digital crime does not even constitute an actual offense. A common example is when a person starts to steal information from sites, or cause damage to, a computer or computer network. This can be entirely virtual in that the information only exists in digital form, and the damage, while real, has no physical consequence other than the machine ceases to function. In some legal systems, intangible property cannot be stolen and the damage must be visible, e.g. as resulting from a blow from a hammer. Where human-centric terminology is used for crimes relying on natural language skills and innate gullibility, definitions have to be modified to ensure that fraudulent behavior remains criminal no matter how it is committed.

Additionally, many states fight international efforts to modify their own internet laws as they feel it is a violation of their sovereign right to police themselves and mete out their own justice. This can be especially problematic when mixed with numerous Western states' attitudes towards terrorism. The United States, for instance, has pledged that regimes that support terror are akin to terrorists themselves and will be opposed. Though this doctrine may be pragmatic when applied to physical terrorism where violence is physically perpetrated, it could potentially destabilize a region if the same doctrine is applied to cyber terrorism. Though this may seem like an outlandish possibility, a large enough act of cyber terrorism could be all it takes to set off major international hostilities.

Additionally, there is a feeling by many lesser-developed countries that combating digital crime could be a misappropriation of their already finite resources. As with maritime piracy, many countries are already engaged in expensive defensive programs aimed at stamping out other forms of terrorism and defending their country's physical resources. Any expenditures to defend their digital resources may not be fiscally possible, especially in light of the contemporary economic slowdown.

Finally, many human rights groups caution against a more regulated Internet for a number of reasons, not the least of which is the violation of personal privacy that may occur as a result of increased monitoring. While different countries have different concepts of personal freedoms and liberties, one uniform solution would not likely satisfy the rights of all people in different countries around the world. For instance, China imposes extremely strict restrictions that would constitute a complete violation of American rights if applied to the United States. Even small measures such as new flexibility in the US' monitoring the Internet activities of its citizens by the Patriot Act and Google's admission that it keeps search records for all its users have been met with harsh criticism. The broad range of perspectives on digital crime and the disparity in laws

and regulations with regards to the internet, which is a non-tangible, intellectual concept to begin with, make combating the issue of digital crime increasingly difficult.

Interpol

The UNODC is clearly the primary UN agency to combat digital crimes but it is vital that the UNODC cooperate with Interpol, the international police agency based out of France. Interpol hosted the 7th International Conference on Cyber-Crime in September 2007 in New Delhi, India. Representatives from many of Interpol's 188 member countries assembled in New Delhi to discuss and coordinate strategies to combat cyber-crime and cyber-terrorism and to draw upon Interpol's signature I-24/7 program that allows all member countries to share essential information about international criminal activity. Integrating Interpol's expertise and existing networks into the UNODC's programs for combating all forms of digital crime is a fundamental step forward for the world community.

Conclusion

In order to formulate a plan to combat digital crime many obstacles must first be overcome; the least of which is international consensus and the determination of whose place it is to police the Internet. Many countries feel that the responsibility falls to individual states and police forces to monitor activity within their own borders. This assumes a certain degree of altruism and that other states have the resources to accomplish such tasks. While many states would undoubtedly attempt to police digital crime in their own countries, the world community is not likely capable of such an independent solution to this problem.

Consensus would be hard to reach without building an international legal framework for the Internet, a concept that would undoubtedly offend the sovereign sensibilities of many countries and civil liberties of many people. For the UNODC to proceed, it must first determine whether policing and combating digital crime falls under the jurisdiction and responsibility of the UNODC, and if so what aspects of digital crime are relevant and which can be left up to individual countries to police. Additionally, the UNODC needs to assess what, if any, measures can be utilized by the international community in combating this nuanced and constantly evolving problem.

Guiding Questions

- 1.) Is Digital Crime an issue that has plagued your nation? What, if any, attacks have been perpetrated against your nations or groups living in your nation?
- 2.) Does your nation rely heavily on internet based services and agencies? Which of these web-related entities could be potentially at risk and does your nation currently employ any web-based security systems for protecting those assets?
- 3.) What initiatives are your country currently pursuing with regard to this issue?

4.) What types of laws and restrictions does your country have in place with regards to the internet? How have these laws changed recently and what is your country's position on an international legal framework with regards to internet activity.

5.) What are the penalties for web-based crimes in your country?

6.) What degree of social freedoms does your country currently offer and how would your citizens respond to legislation that may infringe upon their civil liberties in the context of the internet?

Works Cited

Baranetsky, Victoria (2009) "What is cyberterrorism? Even experts can't agree" Harvard Law Record.

"Defining Malware: FAQ". technet.microsoft.com. Retrieved 2009-09-10.

Denning, Dorothy E. (2000) *Testimony before Special Oversight Panel on Terrorism, US House of Representatives*, Georgetown, Washington DC.

"Estonia fines man for 'cyber war'". BBC. 2008-01-25. Retrieved 2008-02-23.

F-Secure (March 31, 2008). "F-Secure Quarterly Security Wrap-up for the first quarter of 2008". Press release. Retrieved 2008-03-31.

Fafinski, S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan.

Jacobson, Roberta Beach (2001-11-27). "*Copyrights and Wrongs*". www.articlestree.com. Retrieved 2007-04-07.

Kostopoulos, George K. (2008) "Cyberterrorism: The Next Arena of Confrontation" IBIMA Volume 6.

Poulsen, K. (2003, August). Slammer worm crashed Ohio nuke plant network. Security Focus.

Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, Routledge, London.

Weimann, Gabriel (2006). *Terror on the Internet: The New Arena, the New Challenges*. United States Institute of Peace, U.S.

