The final copy of this thesis [dissertation] has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.
How the Internet has Changed the Face of Crime

Sara Norden

Florida Gulf Coast University
# Table of Contents

Abstract ........................................................................................................................................... 3

Background of the Study ............................................................................................................. 6

Statement of the Problem ........................................................................................................... 10

Purpose of the Study ................................................................................................................... 10

Theoretical Framework .............................................................................................................. 10

Hypothesis ..................................................................................................................................... 13

Significance of the Study ............................................................................................................ 13

Definitions of Terms .................................................................................................................. 14

Assumptions and Limitations .................................................................................................... 16

Review of the Literature ............................................................................................................. 16

Methodology ................................................................................................................................. 49

Summary, Conclusions, and Recommendations ........................................................................... 49

References ..................................................................................................................................... 56
Abstract

The Internet and the number of Internet users have grown quicker than anyone ever imagined. As people continue to venture into cyberspace and conduct more of their professional activities online, this has created vast opportunities for cyber crime. These offenses are comprised of new types of crimes and new methods of committing traditional crimes such as identity theft, property crimes, and fraud. The depth of cyberspace allows terrorist organizations to recruit, plan, organize, fundraise, and spread their message through propaganda and other digital means. Millions of people across the globe are affected by online crime every day. Cyber crime has become one of the most threatening and difficult problems for law enforcement, the judicial system and the public at large. Due to limited and often biased research based on small convenience samples, it is difficult to determine the full scope of cyber crimes. This paper reviews various types of cyber crimes and the Internet’s overall effect on the evolution of crime.
How the Internet has Changed the Face of Crime

The Internet is a global system of interconnected computer networks that has revolutionized nearly every aspect of human lives. Internet technology and the development of cyberspace have taken society to the next level of evolution. An integral feature of societal evolution has been the development and use of technology and its associated components. The rapid advancement of the Internet has allowed entire industries to move their operations online. The Internet allows legitimate companies and criminal enterprises to expand their operations globally. The United States accounts for approximately one third of computer ownership in the world. Research shows that more men than women use the Internet, although that gap is closing. The Internet provides a vast array of services and resources that are merely a click away; the world is literally at our fingertips. It has allowed for greater flexibility in working hours and location, enhanced globalization, provided educational material at all levels from pre-school to post-doctoral, provided an alternative medium for experiencing new and creative romantic endeavors, and made collaborative work dramatically easier through the instantaneous sharing of ideas. Although cyber crime is not a new phenomenon, computers have always proved to be lucrative targets; the essentialness of the Internet has necessitated a change in our understanding of security, risks, and threats (Singhal, Tandan, & Miri, 2013). Not only does the greater connectivity increase the number of potential victims of computer-related crime, it also increases the number of prospective offenders (Grabosky, 2000).

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. It has no geographical or political boundaries, and can be accessed from anywhere in the world from a multitude of devices. The Internet is not without its own dangers and problems. The growth of
the Internet has been accompanied by an increase in newly detected system vulnerabilities – insecure areas that may threaten the security of a computer system. Technological advances have always been used to the advantage of criminals. This has led to the development of the field of cyber criminology which is a multidisciplinary field that encompasses researchers from various areas such as criminology, victimology, sociology, Internet science, and computer science (Jaishankar, 2010). Another alternative word that has been used by other professionals is virtual criminology. Cyber criminology is often merged with cyber-forensics. Cyber-forensics deals exclusively with the investigation of cyber crimes, whereas cyber criminology deals with the causation of cyber crimes. It’s a field that is slowly emerging from a niche area that is often marginalized by mainstream criminology to one of high importance.

Traditional cyber crimes are crimes that occur in the physical world but involve technology such as stealing a computer or mobile device with Internet capability. True cyber crimes are crimes that can only be executed in the virtual world, such as phishing and social engineering. Many traditional crimes are now being aided, enhanced or abetted through the use of computers and networks, and wrongdoing previously never imagined has surfaced because of the capabilities of information systems and advanced technology devices (Hinduja, 2007).

Hybrid cyber crimes are crimes that can be committed with or without the internet, but are increased in severity through the use of computer technology such as cyber terrorism and child pornography (Hassan, Lass, & Makinde, 2012). The number of new technologies, especially mobile phones, has increased opportunities for criminal activity. Cyber crime is a worldwide problem that is costing countries billions of dollars. Computer crimes have caused havoc to individuals, private and public business organizations, causing financial, and in some cases, physical and emotional damage. Cyber crime, like other types of criminal activity, can be
associated with high rates of unemployment and harsh economic conditions. Lack of gainful employment allows youth the opportunity to use their time and knowledge as a platform for their criminal activity. There continues to be a large gap between the rich and the average, as many strive to bolster their socioeconomic status using the quickest means possible. Today many parents transmit criminal values and acceptance of deviant behavior to their children. If this culture is entrenched among the younger generations, most of them will see no wrong in cyber crime practices (Hassan et al., 2012).

Estimating the incidence, prevalence, and cost of computer-related crime is a difficult challenge. Research shows cyber crime is a growing worldwide problem and no country is immune. Statistics on computer-related crime are not a true reflection of the number of crimes committed because they are out of date before they appear in print and cyber crime is notoriously underreported. Some of the most skilled perpetrated offenses are never detected. In the United Kingdom in 2006, there were 92,000 cases of online identity fraud. In 2006, 850,000 cases of unwanted online sexual approaches occurred. The systems of NASA, US Army, Navy and Department of Defense were hacked right after the 9/11 attacks (Kamal, Chowdhury, Haque, Chowdhury, & Islam, 2012). In 2012, the Internet Crime Complaint Center (IC3) received 289,874 consumer complaints with an adjusted dollar loss of $525,441,110, which is an 8.3 percent increase in the reported losses since 2011 (Internet Crime Complaint Center [IC3], 2012). The Internet Crime Complaint Center was established in May 2000 to address the increasing incidence of cyber crimes.

**Background of the Study**

The last two decades have shown massive increase in the use of computer technologies in a wide range of business and domestic scenarios. There are few, if any, people in Western
society whose lives are not affected in some way by the use of Information Technology and the Internet. The Internet is not only a tool to use for work, study or pleasure but is a very important part of our life in general. It gives that magic feeling to accomplish things and be invisible, but this invisibility or perceived invisibility, maybe lead to actions someone wouldn’t do in person or in public – actions that might be wrong.

Online crime has taken off as a serious problem since about 2004. Prior to that, much of the online nuisance was from amateur hackers who wrote malicious software and defaced websites in pursuit of bragging rights (Moore, Clayton, & Anderson, 2009). Unfortunately, due to the lax security and ambiguous nature of early information system networks, it is nearly impossible to know when the first Internet crime actually occurred (Henson, Reyns, & Fisher, 2011). The current generations increasingly rely on the Internet and advanced technology to further their criminal operations. Cyber criminals today can easily leverage the Internet and carry out traditional crimes such as trafficking illicit drugs and illegal sex trafficking. Today criminal networks exist with online black markets where trade occurs and criminals are able to take on specialized roles (National Security Council, n.d.). Online criminals are involved in many types of fraud from fake lotteries through stock scams to advance-fee frauds, and in other crimes such as the distribution of images of child sexual abuse. Social networking sites (such as Facebook, Twitter, and MySpace) provide outlets for bullying and stalking. Crimes that were once done in person, like stalking and bullying, have been taken online where the perpetrator can reach their victim twenty-four hours a day, seven days a week.

Thus far, the world has not coped well with the rapid growth and mobilization of online crime. Banks often hide fraud losses, or even blame their customers for fraud, and they hesitate to share information with other banks and law enforcement (Moore et al., 2009). Increased cyber
crime has brought about investigative difficulties because enforcement agencies are ill-equipped to tackle computer crimes because of its technologically-advanced nature and the fact that cyber crime can occur almost instantaneously. Police agencies have floundered from lack of experience in this technical area and the weakness in current legislation that limit the jurisdiction and cooperation of agencies. There are tens of thousands of law enforcement agencies worldwide and many of them are uninformed about computer crime. Existing mechanisms for international police cooperation are designed for rare serious crimes like terrorism and murder, while online crime is petty crime committed on an industrial and global scale. The existing mechanisms for international police cooperation are slow and expensive and are not designed for dealing with online crime. What is specifically illegal varies from one country to another: the leading global legal framework, the Council of Europe Convention on Cybercrime, has been ratified by the United States but has yet to be ratified by a majority of European Union member states. Once nations have agreed on what is a crime, law enforcement agencies will still have little incentive to work together on globalized crime (Moore et al., 2009).

A serious crime that often provokes considerable alarm is cyber terrorism. Cyber terrorism represents the convergence of the virtual world of cyberspace and the intimidation techniques of terrorism. The potential threat of cyber terrorism is alarming and extremely concerning; however, the potential threat posed by cyber terrorism has been exaggerated in the past and leads to confusion over how real the threat actually is. Research shows that cyber terrorism is an attractive option for modern terrorists who value anonymity and the opportunity to inflict massive damage (Weimann, 2004). Cyber terrorism also has media appeal which is important to many terrorist groups. Despite the possible exaggeration of cyber terrorism, there is
still a need to implement legislation and enforcement measures to address and prosecute
perpetrators for planning and organizing a terrorist attack (Prasad, 2012).

Hard statistics on losses from online crime are difficult to come by in most countries. The
cyber crime data available is fragmented due to several causes, one being the reoccurring
argument over what the definition of cyber crime actually is and what should be reported. A
conflict of interest is occurring because many of the statistics on security failure are collected by
parties with an incentive to under or over report. There is a chance that governments might seek
to minimize crime statistics by changing reporting requirements. In a particularly egregious case,
the UK government changed the rules so that fraud must be reported to the bank rather than the
police. This change caused the fraud figures to drop to near zero and was strongly criticized by a
Parliamentary committee (House of Lords Science and Technology Committee, 2007). Without
accurate information on online crime, it is hard for private markets to provide incentives for
more secure software and it is hard for law enforcement professionals and government officials
to grasp the magnitude of this problem. Despite the misinformation and lack of information
surrounding the proliferation of cyber crime, the Federal Bureau of Investigation (FBI) lists
cyber crime as its third priority behind terrorism and counterintelligence.

Responsibility for online crime prevention could be placed on computer owners, software
suppliers, private security firms, law enforcement, Internet service providers, or banks. As
expected, every one of these stakeholders wants someone else to fix the problem. Accountability
and cooperation is a must to combat growing online crime. To control online crime better, a
greater understanding of how online criminal activity works, why current enforcement efforts are
feeble, and an economic perspective of the incentives faced by the different players are
necessary.
Statement of the Problem

Despite the expansive global recession, improved security, and international crackdown efforts, cybercrime has thrived the last decade, growing by double digits year after year. The Internet is an evolving frontier where new criminal threats are consistently emerging. Law enforcement and other criminal justice professionals are struggling to keep up in this consistently changing criminal arena.

Purpose of the Study

The purpose of this study is to explain the varying types of cyber crimes and the role the Internet has played in the evolution of crime.

Theoretical Framework

Cyber crime, like crime in general, may be explained by the conjunction of three factors: motivation, opportunity and the absence of responsible guardianship. K. Jaishankar has developed a theory called “Space Transition Theory” to explain the causation of crimes in cyberspace. The Space Transition Theory is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace (Jaishankar, 2007). This theory argues that people behave differently when they move from one space to another. Some of the postulates of the theory are persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society, and Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime (Jaishankar, 2008).
The Internet has assisted the evolution of new social norms and accepted behaviors. The adherence to copyright laws has drastically decreased with the advent of the Internet. The theft of copyrighted materials via file-sharing website is considered relatively socially acceptable by internet users today. Pirate Bay, MegaUpload, LimeWire, and BearShare are a few of the big file-sharing websites that have been shut down for copyright infringement. It is suggested that poorer nations have higher piracy rates because individuals are less able to afford copyrighted materials and have cultures more conducive to copyright infringement.

Crime does not exist in a vacuum. It has evolved and changed with the times. The literature, broadly defined, is abounding with references to cyber crime and more recently to organized cyber crime. It is difficult to study and conduct research on these topics due to the various terms that are used. One might speak of cyber crime, high tech crime, computer crime, technology crime, digital crime and IT crime and be discussing the same or very different concepts. Achieving any indication of comparative analysis of the impact of cyber crime therefore is filled with difficulties (McCusker, 2006). It is also common to refer to cybercriminal ‘groups’ as if they were of equivalent size, complexity, etc., yet these groups are never defined. Because of these variances, the term cyber crime has rapidly become a generic descriptor for any deviant online behavior no matter what the relative differences in complexity and seriousness are. A recent IBM survey on cyber crime did not define cyber crime and yet sought information from business participants on every continent on the impact of such crime. The net effect of such surveys is that the myth of cyber crime is perpetuated and the facts of cyber crime become sacrificed at the whim of public perception (McCusker, 2006).

Cyber criminals can exhibit a wide range of self interests and motivation, deriving profit, notoriety, societal norms, lack of legal ramifications, and/or gratification from activities such as
hacking, cyber stalking, and online child pornography (Singhal et al., 2013). Current research shows that money is the most compelling motivator behind most cyber crime. The ability to make an impact on large systems may be gratifying in and of itself. Given the degree of technical competence required to commit many types of computer-related crimes, there is an important motivational dimension worth noting and that is the intellectual challenge of mastering complex systems (Grabosky, 2000). Although none of these motivations to commit crime are new, the element of novelty is the ability of technology to facilitate acting on these motivations. In many cases involving cyber crime, human behavior is driven by multiple motivations, both intrinsic and extrinsic.

Ideology is an important component that feeds the behavior of many cyber criminals. A number of cyber attacks are linked with fights for ideology. Ideological hackers attack websites to further political purposes (Kshetri, 2005). The Internet has provided a new venue for stimulating civic participation and engagement. Hackings by Islamic activists and Cyberjihad, a group of hackers in Indonesia, are examples of ideological cyber attacks.

Cyber terrorism can be examined from two perspectives: the technological attack and the psychological motivation driving the threat. In this paper, the latter is examined by discussing various motivating forces that drive terrorism such as theological beliefs which can justify the use of violence and can include the sacrifice of one’s life. Terrorist attacks seek a wide-spread response and by using the media, attacks can be widely publicized. It causes a spotlight to be placed on the group and their message is more widely and quickly distributed.

Scholarly work has generally identified four main contexts that can explain why people commit crimes: biological, psychological, sociopsychological and sociological. Motivations vary depending on the nature of the crime, but may include greed, lust, revenge, challenge or
adventure. These contexts are typically applied to explanations involving violent crime and street crime, but some of these factors can be applied to non-violent criminal activities. The routine activity theory can be used to explain cyber crime by attributing the supply of both motivated offenders and suitable targets for victimization to an increasing internet user population and familiarization with computer technology. Since cyber crime continues to grow at alarming speeds and professionals are still working to understand these crimes, there is a lack of standardization and theoretical framework to guide those working in these fields.

Research suggests that the anonymity of the Internet reduces or mediates inhibition of delinquent behavior, bullying included. Mason (2008) goes on to suggest that the Internet creates a new context for social interaction. Because of these factors, individual identity is replaced with social identity, whereby social norms serve to regulate behavior (Cesaroni, Downing, & Alvi, 2012). Anonymity in cyberspace has changed the mindset of online users in that it decreases their sense of personal accountability and direct association, and therefore contributes to an increased tendency to commit crimes online that they may not typically commit in person.

**Hypothesis**

The advent and subsequent growth of the Internet has changed the face of crime.

**Significance of the Study**

As the Internet gains increasing prominence in the lives of people, it is important to understand how the Internet affects all facets of the way we live, work and play. Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. The ability to share and exchange information immediately has provided unprecedented and unparalleled benefits in the areas of education, business, entertainment and social interaction (Wang & Huang, 2011). On the negative side, it has created increasing
opportunities for the commission of crimes including the proliferation of pornography, hate crimes, cyber stalking and online fraud. This study is significant because criminal justice professionals and other professionals must understand how the Internet has affected the progression and evolution of crime to better understand how to curb the proliferation of online crimes.

**Definitions of Terms**

Internet: The single worldwide computer network that interconnects other computer networks, on which end-user services, such as World Wide Web sites or data archives, are located, enabling data and other information to be exchanged.

Computer dependent crime: A crime which could not exist without new technology. An example of this would be harvesting bank account details through malware (Hargreaves & Prince, 2013).

Computer enabled crime: A traditional crime that is increased in its scale or reach through the use of technology.

Cracker: A person who breaks into other people’s computer systems for fun or who intend to cause harm.

Cyber Crime or Computer Crime: A term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity. Cyber crimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones (Halder & Jaishankar, 2011).
Cyber extortion: A form of online crime which occurs when a person uses the Internet to demand money or other goods or behavior (such as sex), from another person by threatening to inflict harm to his person, his reputation, or his property.

Cyber terrorism: The unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Hacker: A person who accesses a computer system by circumventing its security system or someone who shares an anti-authoritarian approach to software development now associated with the free software movement

Hacktivism: A term that is composed of the words ‘hacking’ and ‘activism’ and is the handle used to describe politically motivated hacking.

Jurisdiction: A government’s general power to exercise authority over persons and things. This general power encompasses three distinct concepts: jurisdiction to prescribe (make laws), jurisdiction to adjudicate and jurisdiction to enforce.

Malware: Malware, short for malicious software, aims to infect computer systems without the owner’s consent.

Pharming: A method of redirecting Internet traffic to a fake website through domain spoofing.

Phishing: A method of fraudulently obtaining personal information, such as passwords, Social Security numbers and credit card details by sending spoofed emails that appear to be sent from trusted sources, such as banks, government officials or legitimate companies.

Spam: The use of electronic messaging systems to send unsolicited bulk messages indiscriminately. A person who creates electronic spam is called a spammer.
Virus: A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission

Worm: A virus that spreads by creating duplicates of itself on other drives, systems or networks. A mass-mailing worm is one that requires a user’s intervention to spread, (e.g., opening an attachment or executing downloaded files. Most of today’s email viruses are worms.)

Assumptions and Limitations

This study is limited by the availability of research on online crime. Statistics on online crime are limited due to the reasons discussed above. Often times people do not realize they’ve been a victim of online crime and these crimes go unreported. Much of the data regarding internet crime is classified and not in public domain, therefore this study is limited to the research that is publicly available.

Technology is changing and evolving rapidly. The information contained in this paper may be outdated by the time of publication.

Review of the Literature

There are many different types of cyber crimes and some of the categories discussed in this section are fraud, hacking, online intrusion, phishing, online pharmacies, drug trafficking, gambling, child pornography, cyber stalking, cyber bullying, and terrorism. These varieties of computer-related crimes are not exclusive, nor is this by any means an exhaustive list.

Since everyday a new dimension of cyber crime is invented and subsequently evolving, it is impossible to fully discuss all types. Online identify theft is one of the biggest and most well known cyber crimes. It’s also the fastest growing. Identity theft involves the misuse of an individual’s personal information without their knowledge or consent for the purposes of committing theft or fraud. Around 40% of all identity frauds are facilitated online (Kamal et al.,
The most stolen documents used by criminals committing fraud were utility bills, passports and bank documents. Once the individual’s personal information is obtained, offenders have the ability to purchase goods or services while posing as the victim. Digital technology also permits perfect reproduction of documents such as birth certificates, identification cards or other documents which may be used to construct a false identity, as well as counterfeiting of currency and other fraudulent instruments (Grabosky, 2000). Due to recently enacted data breach disclosure laws, consumers have begun to learn the scope of the online identity theft problem. Its insidious nature is defined by the anonymity afforded the perpetrators and the devastating impact it has on its victims, compounded by the fact that the economic harm often is not discovered until long after the crime has occurred and the thieves have disappeared (Hoar, 2005). Identity theft can destroy personal credit and potentially lead to very expensive litigation that may take years, or even decades, to correct.

“Phishing,” the act of sending a fake email to an unsuspecting user that appears to be from a legitimate enterprise, is a common method of identity theft. In phishing fraud schemes, a perpetrator poses as a legitimate business, such as an online retailer, bank, or credit card company, in an attempt to get the online user to provide personal information such as passwords and bank account numbers. Some of the more common businesses and industries replicated in phishing scams include banks, online businesses like eBay or Paypal, and online service providers like AOL and Google. Unsuspecting victims receive emails that appear to be from these entities, often suggesting suspicious activity regarding the account and requesting personal information. These phishing emails encourage users to visit fraudulent websites to divulge their sensitive information and all the while the user is none the wiser that they are sharing their information with a fraudster. According to one study, phishing caused approximately $1.2 billion
in direct losses to banks and credit card issuers in the United States in 2003. Gartner, Inc. went on to report that 30 million adult Internet users believed they had recently experienced a phishing attack, while another 27 million suspected they had witnessed a phishing attack (Hoar, 2005). Phishing scams acquire direct information, such as usernames and passwords, often through misrepresentation. Despite phishing schemes being obvious to more technologically savvy and crime knowledgeable people, these expeditions appear to have a high rate of success. Effort is made to make the spam attacks look official by using the names of various government agencies and high-ranking officials to convince individuals to provide personal information so they can then be defrauded. It is important to know that government agencies do not send unsolicited emails. Complaints that use the name of FBI Director Robert Mueller continue to make up a large part of the government impersonation email scams (IC3, 2012). Robert Mueller stepped down on September 4, 2013.

Online intrusion involves the use of the Internet to invade, harm or otherwise infect another user’s online space, computer programs, network, or computer systems (Henson et al., 2011). The most dangerous form is malicious software, also called malware, which is downloaded to an unsuspecting victim’s computer when the user opens an email message, an attachment, or clicks on a hyperlink within the bogus message. It may then disseminate viruses, Trojans, and/or worms designed to harvest the user’s private information. Malware may also be downloaded via peer-to-peer file sharing programs such as BitTorrent or Filesoft or from pirated software. Online piracy is sharing or stealing of intellectual property, and the piracy problem is compounded by peer-to-peer file sharing programs that allow these illegally copied materials to be distributed (Henson et al., 2011).
Back in the early part of the century, most such malicious software’s primary aim was seeking a thrill. The people writing the software found it amusing to challenge themselves by writing a program that could exploit security flaws just to see how far it could spread (Hassan, Lass, & Makinde, 2012). Today the incentive for making such software is generally more malicious and dangerous. Cyber culprits can use networks of these infected computers, or botnets, for malicious activities ranging from attacking bank servers containing private information to automatically sending thousands of simultaneous emails for the purpose of defrauding users (cyber criminology reference). One infected computer can potentially generate 25,000 spam messages per hour or 600,000 per day (Keizer, 2009). The Trojan horse is also a technique for creating an automated form of computer abuse which works on financial data. This technique causes small amounts of assets to be removed one slice at a time from a larger pool. Malware can also have the additional effect of preventing users’ anti-virus and security protection software from updating which exposes the infected machines to even more malicious software. Online identify theft and malware have led to the creation of associations, alliances, working groups, and initiatives involving the largest banks, Internet service providers, technology venders, and law enforcement entities. These groups have united to try to combat cyber crime and pursue a cleanup of the Internet.

Internet fraud refers to any type of fraud occurring online. Fraud is not a new crime, having been around since human history, but the nature of fraud became even more complex with the introduction of Internet communications and electronic commerce. Fraud and theft offenses constitute the biggest proportion of the cyber crimes since the main motivation of the criminals is personal and economic profit (Gul & Terkesli, 2012). Online fraud is costly and takes a great amount of time to restore the harm done. Since the Internet works on real time, a
The various types of Internet fraud parallel those committed offline. While Internet deception is troubling in its own right, its increasing occurrence is a threat to Internet commerce. Consumers around the world are becoming more comfortable with ecommerce practices. An individual’s daily life includes multiple online activities and transactions including shopping and banking. When buyers have trouble deciding between good and bad products, even a small number of deceptive sellers might negatively impact a market, driving out good products and eventually the consumers. This has been an increasing trend with the once extremely popular online auction site eBay. In online auction fraud, the sale of products advertised on the Internet is misrepresented by the seller or the items are never delivered after the victim has appropriately paid. Internet auctions and sale of general merchandise are two of the most popular scams used...
by online scammers. Nigerian money offers also continue to be a popular method of online scamming. The Nigerian schemes, also called a 419 from Section 419 of the Nigerian Criminal Code that addresses fraud schemes, involve convincing the victim to send money to the perpetrator in order to share a large sum of money from a foreign bank account (Henson et al., 2011). The Nigerian Government blames the growing problem of the successful fraud schemes on mass unemployment, extended family systems, and the greed of foreigners that causes them to fall for the scheme in the first place.

According to the Theory of Deception, a deception is a cognitive interaction between two parties under conflict of interest (Johnson, Grazioli, Jamal, & Berryman, 2001). Deception exploits systematic weaknesses in our cognitive systems, and it has been argued that deception is the inevitable price humans must pay to cope with the complexity of the world; a complexity which technology has only increased. Research across various contexts has shown that humans are generally poor detectors of deception which is why these crimes continue to be very successful. Much evidence suggests technology-based fraud is increasing in frequency despite law enforcement efforts. According to a February 2009 Spam report by security software firm Symantec, the presence of spam, ranging in nature from advertising to outright fraud, has spiked since 2008. Results from the National White Collar Crime Center’s 2005 National Public Survey on White Collar Crime noted a “sharp rise” in the number of technology-based white collar crimes, and suggested that technology-based crimes were becoming increasingly prevalent (National White Collar Crime Center, 2006). The increase in fraudulent emails is also supported by a 2008 Microsoft security report which found over 97% of all emails are unwanted and target the small percentage of users who fall prey to seemingly innocuous links and email attachments (Microsoft, 2008). There still remains no governing or professional authority that has the ability
or capability to monitor Web content (Koong et al., 2012). Consumers should utilize the
technology available to closely monitor their accounts for unusual or unexplained transactions.

Scammers also appeal to sympathy and sense of charity. Two notable reasons for
solicitation are illness and social/political victimization. Phishing scams often spike following a
traumatic event such as a natural disaster like Hurricane Katrina. Current research and theory
suggest social engineering or the manipulation of people is the most important part of online
fraud. Spam allows unsolicited bulk messages to reach a wide audience through instant
messaging systems, Internet forums, junk fax transmissions, social networking websites, and file
sharing networks. Spamming remains economically viable because advertisers have no operating
costs beyond the management of their mailing lists, and it is difficult to hold senders accountable
for their mass mailings (Hassan et al., 2012). The emergence of cheap electronic services and
devices has increased spamming. Because the barrier to entry is low, spammers are numerous,
and the volume of unsolicited mail has increased exponentially. Nearly 200 billion spam
messages were sent each day in 2012, double the volume in 2007, and 90% of all emails sent
worldwide are spam (Kamal et al., 2012).

In addition to financial damage, cyber crime victims often suffer from the psychological
discomfort of being victimized, the loss of time necessary to file complaints and refund requests,
and the theft of private information. According to the Federal Trade Commission, 31% of
identity theft victims who had new credit cards taken out in their names required over 40 hours
to rectify credit issues and faced consequences such as harassment by creditors (48%), loan
rejections (25%), and criminal investigations (12%) (www.ftc.gov). Internet fraud not only
harms consumers, but undermines their confidence in legitimate e-commerce and the Internet
which harms business concerns. It is estimated that online fraud cost electronic commerce Web sites $2.6 billion in 2004 – an increase of $700 million over 2003 (Hoar, 2005).

Internet fraud should be examined by considering the environmental conditions that contribute to its proliferation. Researchers have identified several factors as contributing to internet fraud which are ease of access, anonymity, availability of email extraction software, ignorance of the gravity of online crimes, economic conditions, and inadequate law enforcement response. Limited legal response to computer crime further exacerbates social conditions that are conducive to crime. The Internet has reduced the costs of committing fraud while dramatically increasing the base of potential victims. The temptation to reproduce copyrighted material such as movies and music for personal use, for sale at a lower price, or for free distribution has proven irresistible to many (Grabosky, 2000).

Hacking or computer intrusion is the unauthorized access to a computer or other digital processing or storage device. This method of attack has been popularized by movies like Hackers and other mainstream media outlets. Cyber attacks can be classified into two types: targeted and opportunistic attacks (Kshetri, 2005). In a targeted attack, specific tools are used against specific cyber targets after a plan is in place. An opportunistic attack entails releasing worms and viruses that spread indiscriminately across the Internet. The number of targeted cyber attacks is on the rise. Targeted attacks are carried out by skilled hackers, terrorists, rival companies, ideological hackers or government agencies (Kshetri, 2005).

There is a common stereotype that portrays hackers as being young and antisocial, hiding in their basements and preying on unsuspecting computer users. Research has shown that most hackers are young and educated, work independently and do not fit police profiles of criminals (Kshetri, 2005). Mobile telephones are the latest targets for computer intrusion attacks. The first
worms capable of attacking cell phones were detected in 2004. Indications are that these attacks could prove even more prolific and dangerous than those against computers because there are so many more cell phones, and cell phone vendors open their operating platforms to third parties in order to develop Internet accessible applications (Hoar, 2005). Hackers have attacked computer networks of the Pentagon and the White House, NATO’s military websites and have stolen secret source codes of Microsoft and the credit card numbers from a number of U.S. banks (Kshetri, 2005). Often times hackers attack websites of symbolic value such as important government sites. A subcategory of hacking is cyber terrorism which is a growing problem that must be addressed accordingly. Cyber terrorism is discussed in more detail in another portion of this paper. Hacking, as a part of cyber crime, is moving forward with new technology to hack and new viruses to spread that are coming out every day.

One of the most heinous crimes to surface on the Internet is child pornography. It is estimated that child pornography, which generates $3 billion annually, is requested 116,000 times daily through certain peer-to-peer file sharing programs, and is featured on more than 100,000 Web sites (Hoar, 2005). Collections of child pornography do not arise by accident, but by the deliberate choices individuals make to acquire such material. Today illegal pornographic material is imported across national borders at the speed of light. The proliferation of free web servers has meant that perpetrators can upload a website containing child pornography anonymously and with little effort. Child pornography is one of the fastest growing businesses online, and the content is becoming more graphic. In 2010, the Internet Watch Foundation found 1,351 individual child abuse domains. Of all known child abuse domains, 58 percent are housed in the United States (Internet Watch Foundation, 2010). In Britain, during 2008, there were 500 new cases of online child abuse reported every month (Kamal et al., 2012). Technological
changes are evident in the emergence of pornographic material distributed through the Internet, but video still seems to remain the principal primary production medium for child pornography (Taylor, Quayle, & Holland, 2001). The Internet is the principal means of exchange of child pornography. New technologies also mean that people who view child pornography can become people who produce child pornography. Technology allows the user to manipulate images to fit a particular sexual fantasy which further makes the child merely an object of sexual gratification. Technology is also being used to create lifelike child pornography without the use of children at all (Taylor et al., 2001). The knowledge of the risk being taken when downloading illegal material can also serve to heighten arousal.

Children, from toddlers to teens, are now exploited for all those who choose to view these photos and films via the Internet. The Internet has allowed sexual predators to create groups and form relationships with like minded individuals and victimize children in the safety and privacy of their own homes. The Internet allows social connections and virtual communities to increase, while providing a safe haven, also allowing for the control of social distance and intimacy (Taylor et al., 2001). “This functions in a way that allows for the normalization of sexual interest in children and enables engagement through the reduction in outside social contacts that might otherwise challenge the acceptability of the interest” (Taylor et al., 2001, p. 99). The Internet creates a world where users can avoid personal and social responsibility by creating anonymity. Sharing and trading pornographic images acts a form of social reinforcement.

The Wonderland Club was an international network with members in at least fourteen nations ranging from Europe to North America to Australia. Access to the group was password protected and the content contained therein was encrypted (Grabosky, 2000). The investigation had been sparked by a tip-off from United States police investigating the rape of an eight-year-
old girl broadcast live to pedophiles by webcam. Over 750,000 images with over 1,200 unique identifiable faces had been distributed by the Wonderland Club. The police investigation, codenamed “Operation Cathedral,” was coordinated by The National Crime Squad, and resulted in over one hundred arrests around the world and the seizure of over 100,000 images in September 1998 (Grabosky, 2000). In 2011, the Department of Homeland Security prevented $1.5 billion in potential losses through cyber crime investigations and announced charges against 72 individuals for their participation in an international criminal network dedicated to the sexual abuse of children and the creation and dissemination of graphic images and videos of child sexual abuse throughout the world (Department of Homeland Security [DHS], n.d.). U.S. Immigration and Customs Enforcement (ICE) Child Exploitation Section investigates large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of engaging in sex with minors.

It is estimated that 29% of seven to seventeen year olds would freely give out their home address to an online friend. The Internet also gives young people easy access to adult oriented material. The average age of a child’s first Internet exposure to pornography is eleven years old. It is difficult to combat this growing problem because parents are often unaware of a child’s activity while on the Internet. Child pornography cases are often made when law enforcement agents pose as participants in Internet user groups or chat rooms where pornographic photos and videos have been posted.

Child victimization in the form of sexual abuse has been an important focus of study for several decades prior to the creation and existence of the Internet. Research has shown that most offenders in non-Internet or conventional child sexual abuse cases perpetrate their crimes against victims within their own families or with whom they are acquainted (Finkelhor, 1997). The
typical stereotype of Internet sex crimes involves unknown adults meeting juvenile victims online. The Internet can also play a major role in sexual crimes against minors by family members and acquaintances. In a 2005 study, data were collected from a national sample of law enforcement agencies about arrests for Internet-related sex crimes against minors. Family and acquaintance offenders were nearly as numerous as offenders who used the Internet to meet victims online. Online sexual exploitation of children occurs when a predator uses the Internet to establish online relationships with children, usually with the goal of taking the relationship into the physical world and meeting the children in person to continue their relationship (Henson et al., 2011). The Internet is used in various ways to further their crimes including as a tool to seduce or groom, store and disseminate sexual images of victims, arrange meetings and communicate, reward victims, or advertise and sell victims. A certain level of anonymity exists online that allows for exploration of sexual interests and affect sexual expression. The Internet allows for private conversation with minors and private access to pornographic material that is often used in these crimes (Mitchell, Finkelhor, & Wolak, 2005). Law enforcement should investigate the possibility of all means of communication between the victim and offender in the context of all child sexual abuse cases including through the Internet. Identifying an Internet component may result in better evidence in the forms of chat conversations or sexual images. Mental health professionals should ask about Internet involvement when working with victims and offenders involved in child sexual abuse cases. A complete understanding of Internet involvement could aid in the development of more effective treatment and future prevention strategies.

Hates crimes were once tied to geography of the place, but now due to modern technologies, their proliferation has defied boundaries (Jaishankar, 2008). Cyber hate was once
confined to chat rooms and emails, but social networking websites are now being used as the medium to spread hate. Sites like Myspace, Facebook and Twitter are being misused to spread hate and cyber bullying. Cyber bullying is a phenomenon that children and adolescents seem to be increasingly using to harm others (Jaishankar, 2008). The growth of cyberspace harassment has been recognized as far back as 1999 with a report from the United States Attorney General to the former Vice President Al Gore, suggesting that incidents were an increasing problem for law enforcement officials (Beckerman & Nocero, 2003). It is difficult to estimate with any precision the extent of the cyber bullying phenomenon. There are significant variances in the available statistics related to cyber bullying, and it is believed this is because the prevalence rates are influenced by sampling characteristics and the types of technology used in question (Cesaroni et al., 2012). In the case of cyber bullying, it seems girls could be more involved than boys as they are more likely to communicate regularly by email and texting. In general, girls inflict virtual abuse more than boys through instant messaging, online conversations, and emails. A survey of girls ages 12-18 found that 74% of adolescent girls spend the majority of their time online in chat rooms or sending instant messages and email (Migliore, 2003). Boys are more likely to make online threats and build websites targeting others. It can be much more difficult to identify bullies in cyberspace. With no boundaries or tangible consequences, children are using technology to vent normal frustrations in ways that can become very destructive (Keith & Martin, 2005).

Cyber bullying is a relatively new form of bullying that is receiving more and more attention in the research literature, public debates and in the media in light of recent events. Bullying has evolved from a few hurtful remarks communicated in person to multimedia interaction that can be communicated via multiple electronic sources (Hendricks, Lumadue, &
The growth of technology and the evolution of the Internet are the foundation and method of communication for cyber bullying. Tragic stories of cyber bullying among children and young adults appear to be becoming more frequent. This problem is not confined to America. Cyber bullying affects all races and is an issue across the globe. There is a growing concern voiced by parents, schools and the public about youth peer harassment via the Internet. Internet use has expanded over the last ten years to encompass nearly all youth, and the nature of youth Internet use changed during this time, with an increase in the use of cell phones and smartphones, and the migration of adolescent social activity to social networking sites such as Twitter and FaceBook (Jones, Mitchell, & Finkelhor, 2013). It has been suggested that the nature of the online environment may influence an increasing number of youth to engage in peer harassment and bullying. Research suggests that cyber bullying may be closely linked to traditional youth deviance, and recent responses to this new problem have ranged from informal education to formal policy debates (Cesaroni et al., 2012). One of the main reasons for traditional bullying is something about the victim that they cannot change or correct such as disliking someone for their hair color, body size, or sexual orientation. It is difficult to develop interventions because the motivations and goals of those who cyber bully are still relatively unknown. The reward for engaging in cyber bullying is often delayed (in contrast to face-to-face interactions), and this is anticipated to have an effect on how goals for these aggressive interactions are formed and pursued (Dooley, Pyzalski, & Cross, 2009).

It also appears that cyber bullies are older as younger children do not use technology for communication with their peers as much as older students. Over 80 percent of teens use a cell phone regularly, making it the most popular form of technology and a common medium for cyber bullying. There is limited research on the consequences of cyber bullying, but the
consequences of face-to-face bullying have been shown to increase levels of depression, anxiety and psychosomatic symptoms in victims. It has been suggested that one of the distinguishing features of cyber bullying is the inability of victims to get away from it. Cyber bullying allows for a public forum and the victim to be publicly humiliated even though the words are typed onto a screen and transmitted through a technology device. In a world where we are always digitally connected through social media and the Internet, young people are constantly bombarded with status updates and other messages from their friends and peers. Within seconds, a rumor can circulate around the school, community or social group before anyone has verified its validity (Hendricks et al., 2012). Written words that occur in cyber bulling may seem more concrete and real than spoken words. These words can be read over and over. The inability to have any control over acts of bullying may result in feelings of powerlessness in the person being bullied. Victims of cyber bullying are often afflicted with intense emotional and psychological pain. Many of the victims experience at least one or a combination of feelings of isolation, embarrassment and shame (Hendricks et al., 2012). Conceptualizing and assessing power imbalance in cyber-based interactions is even more complicated than in traditional forms of bullying (Dooley et al., 2009). Online communication amongst children is often unknown by adults and conducted away from their supervision. This makes it difficult for parents and school administrators to both understand the nature of the problem and do something about it. Extreme cases of cyber bullying have led some young people to commit suicide.

Much work is being done toward modifying the roles and responsibilities of schools, law enforcement, and even technology companies around online safety concerns, and it is critical that these efforts are based on research instead of untested, hurried assumptions (Jones et al., 2013). Schools must implement evidence-based protocols and training for teachers, students, and
parents. It is important to guide children to use technology in ways that promote respect, understanding, and responsibility to lessen the impact of this new form of bullying. Despite the seriousness of cyber bullying, the extent to which cyber bullying is perceived by youth themselves is far less problematic and abnormal than public and scholarly commentaries have suggested (Cesaroni et al., 2012). It is currently unclear if the policies and prevention initiatives that address conventional bullying are sufficient and effective for technology-related harassment. This is an area that warrants further inquiry.

It should be noted that children are not the only ones who face cyber bullying. This Internet phenomenon is something that many adults experience in the workplace and the effects can be just as damaging. In workplace bullying, it is often subtle and undetected for some time. Bullying in the workplace can lead to increased turnover and decrease the commitment of employees (Hendricks et al., 2012). Many cases of workplace bullying have led to physical illness such as high blood pressure and insomnia and psychological trauma in the victim. The bullying is not only harmful to the victim, but it can also decrease the productivity of the workplace and decrease job satisfaction. Workplace bullying should be addressed by management and human resources quickly and effectively to prevent a negative impact on the workplace.

Cyber stalking is another form of computer related crime that has been increasing. Cyber stalking is when a person is followed and pursued online. It is using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. This term is used interchangeably with online harassment and online abuse. The first case of cyber stalking was prosecuted in California in January 1999 after Gary Dellapenta, a 50-year-old security guard, spent the better part of 1998 terrorizing a woman
who rejected his advances (Henson et al., 2011). Dellapenta, posing as the 28-year-old woman, made posts on America Online chat rooms saying she had an unfulfilled sexual fantasy of being raped. The posts included her name, address, phone number, and instructions for disarming her home-security system. Six different men came to her apartment over the course of five months. Luckily none of those men gained access to her apartment. Dellapenta was sentenced to six years in prison.

A cyber stalker typically does not present a direct physical threat to a victim, but follows the victim’s online activity to gather information and make threats or other forms of verbal intimidation. A victim’s privacy is invaded, their every move is watched. Cyber stalking usually occurs with women who are stalked by men or children who are stalked by adult predators or pedophiles. It is believed that over 75% of the victims are female, but sometimes men are also stalked. The anonymity of online interaction reduces the chance of identification and makes cyber stalking more common than physical stalking. Stalkers can more comprehensively use the Internet in order to slander and endanger their victims. Although cyber stalking might seem relatively harmless, it can cause victims psychological and emotional harm, and it may lead to actual stalking in the physical realm. The three primary ways in which cyber stalking is conducted are email stalking, Internet stalking and computer stalking (unauthorized control of another person’s computer). In many ways, stalking via email represents the closest replication of traditional stalking patterns. It is important to note that sending viruses or telemarketing solicitations alone do not constitute stalking. Stalkers are generally of a more mature age than other clinical and offender populations and stalkers usually have attained a greater education achievement than other types of offenders. Women are becoming a more likely cyber stalker with the percentage of known female cyber stalkers increasing from 25% to 40% in 2004 (Keith
Cyber stalking is becoming a common tactic in racism, and other expressions of bigotry and hate. Local law enforcement agencies are beginning to see cases of cyber stalking and some cases have been referred to the U.S. Attorney’s Offices for possible action. The effects of stalking upon an individual may include behavioral, psychological, and social aspects. These effects have the potential to produce a large drain on both criminal justice resources and the health care system, which is why it is important to take swift action when cases are presented and to fully understand this issue. As the Internet continues to grow, problems like cyber stalking will continue to increase. While the behavior of stalking is not new, its recognition in legal and academic circles, especially when the stalking is conducted online, is still in its infancy. Cyber stalking is often seen in conjunction with cyber bullying.

Online pharmacies provide patients with an appealing alternative to the local pharmacy and are attracting a growing number of patients to their sites. Online pharmacies offer some benefits to consumers such as being more accessible to people with limited mobility and to people in remote areas and offer mailed delivery of medications. There is the potential for reduced cost medication. These online pharmacies have triggered reexamination of the ethical, legal, and safety issues involved in prescribing and dispensing medications. The development of online pharmacies has prompted regulatory and monitoring actions at the federal, state, and professional organization levels. This is currently an area of much controversy. Legitimate sites appear to have appropriate technology to ensure security. There is always a certain amount of risk when using the Internet, and there is the potential for data intrusion.

In addition to online pharmacies, drug trafficking deals often take place online. Drug trafficking is the global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law (Hassan et al., 2012). Drug traffickers are
taking advantage of the Internet to sell their illegal substances through encrypted email and restricted-access chat rooms. It is believed that the rise in Internet drug trades is due to the lack of face-to-face communication. These virtual exchanges allow more timid individuals to purchase illegal drugs. This is a growing global problem. The European Commission recently acknowledged the difficulties combating online drug trafficking. It says the complexity and constant innovation by criminals added to the diversity of illegal substances circulating in the European market makes the job increasingly hard ("Online drug trafficking," 2013).

The Internet has allowed miscreants of all types to band together and establish and bustling underground economy. Underground markets that provide buyers and sellers with a meeting place to buy, sell, and trade goods and services in support of activities such as credit card fraud, identity theft, spamming, phishing, online credit theft, and the sale of compromised hosts represent a significant security threat. Previous approaches for disrupting underground markets have focused on standard law enforcement intervention such as identifying and arresting market participants and locating and disabling host infrastructure. These techniques face numerous social and technological hurdles which limit their success and result in substantial associated costs (Franklin & Paxson, 2007). Due to the international nature of these crimes, countries may refuse to cooperate with foreign law enforcement agencies or may lack appropriate laws for prosecution. Without having the computer from which the perpetrator committed the crime then it is very hard to prosecute and convict these wrongdoers. Underground markets should be tracked to allow for accurate forecasting and predictions of the future state of Internet security.

Internet gambling is an area that is ripe with controversy. It has presented a wide range of challenges pertaining to its acceptability by world governments, regulation of use and potential
for abuse. Despite its global impact, Internet gambling is primarily utilized by American citizens (Fidelie, 2009). Studies have shown that when participating in gambling activities, people prefer small, intimate gatherings. This preference leads to more pathological gambling behavior associated with Internet gambling than with a casino because people feel most comfortable in their own home. When someone is engaging in this activity in their own home, there is little incentive to stop. Internet gambling’s interstate and international scope necessitates its governance by federal law. The approach currently used by the U.S. is to prohibit all Internet gambling. The Unlawful Internet Gambling Enforcement Act which was passed in 2006 has proven largely ineffective in providing guidance on Internet gambling regulation, and has failed to successfully prohibit online gambling. Some societal issues associated with Internet gambling are an increase in compulsive gambling, abuse by minors, money laundering, and the proliferation of cyber crimes (Fidelie, 2009). Since prohibition has proven ineffective, there is discussion about whether it may be prudent for governments to allow online gambling and subject businesses to regulation and taxation. Regulation of Internet gambling presents significant challenges in obtaining jurisdiction over a dispute, making an appropriate choice of law, and enforcing judgments rendered by a court. Gambling has long been considered a victimless crime, in that all the people who take part in the illegal transaction are willing participants. Increases in hacking, identity theft, stalking, and cyber extortion have shown that while the Internet is a tremendous invention with many advantageous uses, the crimes associated with its use have taken a toll on society.

The Internet poses new challenges for victims, law enforcement, and lawmakers. Many differences confronting legal efforts to combat cyber crimes are associated with the transnational character of these crimes. It is important to have international legal instruments ready to serve
anti-crime efforts. Legislation that combats computer crime is continuously emerging and evolving as technological advances create the need for additional legislation and the revision of existing laws. The inter-jurisdictional nature of most computer crime provides challenges not found in many traditional forms of criminal behavior. The overlapping hierarchy of law enforcement agencies makes collaboration difficult. In 2006, the United States became an official participant of the Convention on Cybercrime Treaty established by the Council of Europe in an effort to set minimum standards on international cyber laws. The significance and severity of and increasing frequency with which electronic crimes are committed show additional research efforts in this area are needed.

War, crime and terrorism are traditional concepts that occur in the physical domain and are topics that have been explored through scholarly research. The only new aspect is the “cyber” domain. Several researchers have argued that the underlying principles of terrorism behind the threat remain the same, and they have described terrorism activities in the cyber world as cyber terrorism (Ahmad & Yunos, 2012). The term cyber terrorism was first said in the 1980s by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. According to Collin, the convergence of the “virtual world” and the “physical world” form the vehicle of cyber terrorism. Collin further elucidates that the virtual world is the place in which computer programs function and data moves whereas the physical world is the place in which we live and function (Collin, 1996).

Cyber terrorists and cyber warfare passes the threshold of other cyber activities such as hacking, spamming and phishing. These attacks, although seemingly infrequent, are not outside the realm of possibility. In 2007, during an attempt by Russia to punish Estonia for its decision to remove a WW II Soviet War Memorial from the center of Tallinn, Russia launched a series of
cyber attacks that “crashed” Estonia’s Internet infrastructure for over three days. These attacks effectively disrupted banking, business, parliament, news broadcasters, and other important websites. In 2008, during the Russian military conflict with Georgia, Russia employed cyber attack measures against state and private targets in Georgia as part of the Russian military campaign (Bachmann, 2011). Other attacks involved the denial of services to numerous Georgian and Azerbaijani websites. The attacks triggered a number of military organizations around the world to reconsider the importance of network security.

Cyber terrorists target systems that are predominantly operated and controlled by computers. These systems could include critical infrastructure such as utilities (water, electricity, and gas supplies), air-traffic control systems, banking and finance, telecommunications and transport systems (Prasad, 2012). Cyberterrorism presents extreme risks and danger for critical infrastructure and most countries are painfully ill-equipped to prevent or even respond to such an attack. In 2010, the Stuxnet worm virus that targeted the Siemens control systems which were used in Iran’s uranium enrichment centrifuges could have had potentially dangerous consequences for the population, neighboring states and other countries worldwide (Prasad, 2012). Studies show that the Stuxnet virus also impacted computer networks controlling utilities in distant countries including United States, Indonesia, India, Azerbaijan, Pakistan, etc. (Symantec, 2010). The potential of Stuxnet in terms of technical advancement, possibilities and capabilities is enormous: viruses that target industrial systems and actively disrupt industrial processes pose a significant threat to the infrastructure of any developed state (Bachmann, 2011). The Iran operation was considered a covert action, run by intelligence agencies, though many techniques used to manipulate Iran’s computer controllers would be common to a military
HOW THE INTERNET HAS CHANGED THE FACE OF CRIME

program. These threats led the United States and the United Kingdom to respond by establishing a framework of risk mitigation and possible counter techniques.

Internet technology can easily be exploited for the purposes of terrorism in five main ways which include propaganda, recruitment and training, communication, fundraising, and targeting and planning. One of the primary uses of the Internet by terrorists is for the dissemination of propaganda. Examples of propaganda include virtual messages, presentations, magazines, audio and video files and video games developed by terrorist organizations or sympathizers (United Nations Office on Drugs and Crime [UNODC], 2012). Content that might have been distributed to a relatively limited audience in person or by physical media such as compact discs (CDs) and digital video discs (DVDs) has increasingly migrated to the Internet where the ability to reach a large audience is limitless. Terrorist websites often post videos of successful attacks and global American targets creating heroes such as the “‘Bagdad Sniper’ and the ‘Sniper of Fallujah’.” The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content (UNODC, 2012). Terrorists often post messages portraying themselves as victims seeking a peaceful resolution to gain sympathy and claim they were forced into acts of violence after having no other options. Terrorist websites make heavy use of slogans and offer items for sale, including T-shirts, badges, flags, and videotapes and audiocassettes, all evidently aimed at sympathizers. Often, an organization will target its local supporters with a site in the local language and will provide detailed information about the activities and internal politics of the organization, its allies, and its competitors (Weimann, 2005). The promotion of violence and extremist rhetoric encouraging violent acts is a common theme in terrorism-related propaganda. The Internet may be a particularly effective medium for the recruitment of minors, who comprise a high proportion of
web users. Terrorist groups have created video games that target children and young people that encourage the user to engage in role-play by acting the part of a virtual terrorist and perpetrate acts of terrorism and violence. These video games are often offered in multiple languages to reach a broad audience. Terrorist organizations have also used tactics such as mixing cartoons and children’s stories with messages promoting and glorifying acts of terrorism, such as suicide attacks (UNODC, 2012). Propaganda aimed at supporters or potential recruits may be focused on radicalization and incitement to terrorism through messages conveying pride, accomplishment and dedication to an extremist goal. Websites are easily customizable and terrorist propaganda often targets and is tailored to appeal to the vulnerable, isolated and disenfranchised. Possible recruits are spotted by lurking recruiters who, through gradual encouragement of discussion of religious issues, start to slowly include more political discussions. Propaganda can be easily adapted to account for demographic factors, such as age or gender, as well as social or economic circumstances (UNODC, 2012). Besides normal propaganda messages, the al-Qaeda also offers a library service which holds over 3,000 books and monographs from “respected jihadi thinkers” which can be easily accessed and downloaded to mobile phones.

Terrorist organizations often use the Internet to finance acts of terrorism. One of the primary ways that terrorist organizations use the Internet to raise funds is through criminal activity. Many of the methods employed by these groups have been discussed in this paper such as online gambling sites, online payment facility exploitation, and charities and Non-Governmental Organizations (NGOs) with ties to terrorist groups. Charities and NGOs are a common fundraising tactic favored by the al-Qaeda and Hamas. Some charities are founded with the sole purpose of financing terrorism activities, while others are existing entities that are infiltrated by terrorist operatives and supporters and co-opted from within (Jacobson, 2009).
Many of the terrorist-linked charities have had websites openly advertising their activities and soliciting funds. This includes the Global Relief Foundation (GRF), an organization designated in 2002 by the U.S. Treasury Department for its ties to al-Qaeda (Jacobson, 2009). GRF’s mission statement focused on its work in emergency relief, medical aid, advancement of education and development of social welfare. GRF accepted donations by credit and debit cards and wire transfers directly through its website until it was raided and shut down on December 14, 2001. According to the Treasury Department, the GRF helped fund a number of terrorist activities, including bombings of the U.S. embassies in Kenya and Tanzania and armed action against groups perceived to be un-Islamic. Other examples of overtly charitable organizations used for terrorist ends include the Benevolence International Foundation and the Holy Land Foundation for Relief and Development. Combating these fraudulent charities pose unique problems for law enforcement officials because an exposed charity tied to terrorism can be shut down one day and reopen the next under a new name in another county, making them extremely difficult to effectively dismantle. Online gambling sites and other similar entities have also made it easier to launder money on the Internet than it was in the past (Jacobson, 2009). Many terrorist organizations have taken advantage of the Internet opportunities in recent years. Another fact that is likely fueling the increase in terrorists’ criminal activity on the Internet is that key terrorist leaders and operatives have specifically encouraged their followers to pursue this path to protect their anonymity (Jacobson, 2009).

The anonymity the Internet offers provides a certain level of security to terrorist organizations. Encryption software provides instant security so terrorists are able to send messages across the world. Some terrorist websites are actually hosted by companies in the United States. These websites are appealing, experts say, because of the high quality, ease of
HOW THE INTERNET HAS CHANGED THE FACE OF CRIME

setup, and low costs (Jacobson, 2009). Legal obstacles also make it hard to listen in on communications or seize communications of possible terrorist groups. The sheer number of Internet users ensures it is impossible to monitor the majority of people who utilize the Internet for nefarious purposes.

The Internet provides virtual training camps for terrorist organizations that are much like online classes offered by universities and other learning institutions. There is a growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice (UNODC, 2012). These Internet platforms can also provide detailed instructions such as how to construct explosives or other hazardous materials for use in a terrorist attack. *Inspire* is an English language online magazine reported to be published by the organization al-Qaeda in the Arabian Peninsula (AQAP) with the stated objective of enabling Muslims to train for jihad at home. This magazine is another example of the many ways the al-Qaeda used the Internet to reach its followers and engage possible recruits. Boston Marathon bombing suspect, Dzokhar Tsarnaev, has admitted to investigators that he and his brother Tamerlan learned to make pressure cooker bombs by reading *Inspire*, which ran a detailed feature about explosive-building in its debut issue in 2010 under the headline "Make a Bomb in the Kitchen of Your Mom" (Jefferson, 2013). Message boards and chat rooms allow terrorists in training to post questions and receive quick responses and instructions from experts.

Another form of cyber terrorism is cyber extortion. This occurs when a website, email server, or computer system is put under attack by hackers by denying services and demanding random in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to function and demanding payments to restore their service (Hassan et al.,
These attacks often involve criminals living in cyber crime tolerant countries around the world. Despite the fact that cyber extortion is growing in frequency and intensity, many victims are companies and are hesitant to contact the authorities for fear that bad publicity may damage their reputation or that rivals may use the situation for their own advantage. The most dangerous aspect of cyber crime is that the victims fail to acknowledge the cause of their unfortunate fate. Not only should victims report any sort of suspicion and/or crime, but the victim needs to identify the suspected machine so police can confiscate it in order to have evidence gathered from the hard drive and Internet cache files (Kamal et al., 2012).

In South Korea in October 2011, a distributed denial-of-service (DDoS) attack was used to disrupt the country's National Election Commission website on the day of a Seoul mayoral by-election. "Information on polling stations was made unavailable during morning hours when a large proportion of young, liberal-leaning constituents were expected to vote en route to work," according to a Freedom House report (South Korea, 2012). There were speculations that these attacks were politically motivated and intended to sway the election for the conservative party. In December 2011, the personal assistant to ruling party lawmaker Choi Gu-Shik was arrested for his involvement; however, further arrests were never made despite public outcry. Police claim the assistant acted alone. In August 2013, China has said it has suffered its "biggest ever" cyber attack, causing many websites based in the country to go temporarily offline. The distributed denial of service attack was said to have targeted servers responsible for sites with a ".cn" domain name. Another example of a cyber attack occurred in Israel in January 2012 and involved the targeting of multiple symbolic Israeli websites, such as the websites of the Tel Aviv Stock Exchange and the national airline, and the unauthorized disclosure of the credit card and account details of thousands of Israeli nationals (UNODC, 2012).
In January 2012, one of WIT Walchi Innovation Technologies programmers (and minority shareholders), Jerome Westrick, allegedly broke into the company’s computer system, changed access codes and passwords, and effectively locked out the company and its customers from getting into the company’s information system. Walchi alleged that Westrick asked for $300,000 in order to reveal the changed codes and passwords (Wlasuk, 2012). Although this plot was eventually thwarted by court intervention, it still shows that these attacks are possible and the variations of this scheme are endless.

Mandiant, a Virginia-based U.S. cyber security firm that tracks hundreds of cyber spying cases around the world since 2004, has said that a secretive branch of China’s military, Unit 61398, is suspected in a significant number of breaches and may have already “systematically stolen hundreds of terabytes of data” from at least 141 organizations around the world (Mandiant, 2013). The Virginia-based company says its seven-year investigation revealed that more than 90% of APT1’s cyber attacks originated from the neighborhood of the 12-story PLA building. Mandiant has opined that Unit 61398 is staffed by hundreds, and perhaps thousands of individuals based on the size of the building and the organization of the attacks. It is suspected that the data was stolen from organizations mostly within the United States. Of the 141 victims found, 87% are headquartered in countries where English is the native language. China’s foreign ministry has vehemently denied these allegations. Recent China-based hacking attempts on high-profile U.S. media outlets, including the New York Times and Wall Street Journal, have revived concerns about cyber espionage particularly with regards to China (Gallo, 2013). This year Washington increased the size of its own cyber security force by more than 4,000 people - an increase from the current 900.
Many criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology (UNODC, 2012). Terrorists have become increasingly sophisticated at exploiting communications technologies for anonymous communication. It is known that online activities substantially improve the ability of such terrorist groups to raise funds, plan attacks, lure new faithful members, and reach a mass audience. The most popular terrorist sites draw tens of thousands of visitors each month (Conway, 2002). The Internet provides a unique opportunity to data mine and is utilized by terrorists to gather any information that may be relevant to their cause or to future operations—such as satellite images, maps and blueprints of future targets (United Nations Interregional Crime and Justice Research Institute [UNICRI], n.d.). Terrorist groups can learn from the Internet a wide variety of details about targets such as transportation facilities, nuclear power plants, public buildings, airports, and ports, and even about counterterrorism measures. Web searches for news articles and other research can easily show weak links in the Transportation Security Administration’s (TSA) airport security and in border patrol and customs. Following the coordinated 2008 terrorist attacks in Mumbai, it was revealed that the Lashkar-e Taibas used Google Maps, Google Earth and GPS to coordinate their beach landing by passing security forces and gaining access to India.

Cyber terrorists have the ability to operate in a borderless environment with the knowledge that there is no single international legislation to stop them. There are increasingly sophisticated technologies available that increase the difficulty of identifying message originators, recipients and the content of Internet communications (UNODC, 2012). Many encryption tools and anonymizing software are available for download on the Internet for free. The Internet connects not only members of the same terrorist organizations but also members of
different groups. For instance, dozens of sites exist that express support for terrorism conducted in the name of jihad. These sites and related forums permit terrorists in places such as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions but also practical information about how to build bombs, establish terror cells, and carry out attacks (Weimann, 2005).

As with combating child pornography, there are many uses of the Internet for countering terrorist activity. Terrorists’ use of the Internet provides opportunities for gathering intelligence and other activities to prevent and counter acts of terrorism, as well as for gathering evidence for the prosecution of such acts (UNODC, 2012). A significant amount of knowledge about the function, activities, members and sometimes the targets of terrorist groups is derived from chat rooms, websites, blogs and other online communications. Strategic communications that provide counter-narratives to terrorist propaganda may also be disseminated via the Internet, in multiple languages, to reach a broad, geographically diverse audience (UNODC, 2012). The Center for Strategic Counterterrorism Communications (CSCC) was established at the direction of the President Obama and the Secretary of State to coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism, particularly al-Qaeda and its affiliates and adherents. The Digital Outreach Team of the CSCC actively and openly engages in Arabic, Urdu, Punjabi, and Somali to counter terrorist propaganda and misinformation about the United States across a wide variety of interactive digital environments that had previously been ceded to extremists (Center for Strategic Counterterrorism Communications [CSCC], n.d.). The CSCC uses websites and media platforms such as Facebook and YouTube for counter-narrative communications. It is important to remember when utilizing the Internet to counter terrorism that safeguards must be in place to prevent abuse of secret
surveillance tools. Any personal data collected must be adequately protected to ensure against unlawful or arbitrary access, disclosure or use (UNODC, 2012).

Some laws have been developed and passed over the past decade in the United States related to Internet use. Mainly the laws address access to data remotely and computing since it poses great threat not only to business but also to public citizens (Muthama, 2013). These laws include the computer Fraud Act from 1978, Electronic communications Privacy Act (ECPA) that was passed in 1986 which ensures the privacy of email, and the Telecommunication Act which regulates content and nature of the information placed in the Internet and conveyed through the same. These laws were merely fledgling attempts to address the problems brought about by cyber crime. The USA Patriot Act of 2001 has aided in investigating and prosecuting computer-related crimes. Prior to the Patriot Act, Internet service providers were limited in their ability to provide information to law enforcement. The Act expands the circumstances under which service providers can now notify law enforcement of suspicious information. For example: when the service provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay (Podgor, 2002).” The Patriot Act increases the penalties for those who cause damage to protected computers such as those located in military bases and government buildings. These penalties are not restricted to completed offenses, but also include attempts. The Act also redefines a "protected computer" to include those that are located outside the United States. Perhaps one of the biggest changes the Patriot Act created was defining computer crimes as acts of terrorism with penalties of up to twenty years in prison. To meet the definition of terrorism, a computer crime will require that the action be knowingly committed and the damage intentional (Podgor, 2002). The Patriot Act and the Gramm Leach Bliley (GLB) Act, also known as the Financial
Services Modernization Act of 1999, required new security measures including customer identification and privacy protection. The United States is not the only country enacting more stringent computer crime legislation. In 2004, South Korea’s National Cyber Security Center has mandated that all Internet-related hacking incidents be reported (Kshetri, 2005). Despite enacting stricter penalties for committing cyber crime, the deterrent factor is minimal since the probability of arrest is low because conventional law enforcement authorities lack skills required in dealing with such crimes. Eastern Europe and Russia are known to have weak cyber crime laws which have provided a fertile ground for computer crimes (Kshetri, 2005). Countries that do have cyber crime laws often lack enforcement mechanisms and the resources to combat these complicated crimes. In May 2009, President Obama declared the United States’ digital infrastructure as a strategic national asset, recognizing that protecting the networks and computers that deliver essential services such as oil and gas, power, and water is a national security priority (Executive Order on Cybersecurity, 2013). On February 13, 2013, President Obama signed an Executive Order 13636 on cyber security to strengthen the security and resilience of critical infrastructure to protect against evolving threats. This order was met with significant bipartisan agreement. The Executive Order included new information sharing programs to provide classified and unclassified threat and attack information to U.S. companies and directed the National Institute of Standards and Technology to lead in the development of a framework to reduce cyber risks to critical infrastructure (Executive Order on Cybersecurity, 2013). The Framework uses expert input to set out voluntary standards and industry best practices to address cyber risks and potential threats to critical infrastructures. The Executive Order also called for a review of existing cyber security regulations to see if these regulations provide sufficient security. Many of
the existing regulations are dated and likely not up to date with current cyber threats and evolving technologies.

Cyber crime presents unique challenges to lawmakers. Over-regulation may stifle commercial and technological development so legislation must be constructed to prevent crime without blocking advancement in the technology fields. It has been argued that in some contexts, the marketplace may be able to provide more efficient solutions to the problems of computer-related crime than state interventions (Grabosky, 2000). Executive Order 13636 also called for a comprehensive research and development plan for critical infrastructure to guide the government’s effort to enhance and encourage market-based innovation which shows the government is aware of the difficulties of balancing regulation and cyber security interaction while encouraging business development and free trade. State laws on cyber crime vary from state to state making it difficult to review each piece of legislation that deals with computer crimes.

Not only has the Internet changed the way crimes are committed, it has also changed how investigators and law enforcement personnel fight crime. The Internet has provided law enforcement with new opportunities to apprehend sex offenders. For example, police can impersonate children in cyberspace in a way they could not in a prior era (Mitchell, Wolak, Finkelhor, & Jones, 2011). Since 1995, FBI agents have been going undercover on websites, blogs, and chat rooms in an effort to catch child predators. These enforcement efforts have resulted in the arrest and conviction of almost 7,000 offenders in the United States (Henson et al., 2011). The active, online presence of undercover law enforcement personnel may also act as a deterrent to others who may be considering similar offenses. Online undercover investigators have the ability to target offenders who download, trade, or sell child pornography via the
Internet. The Internet allows law enforcement to identify and arrest potential offenders against children, hopefully before victimization occurs. As with other types of online crimes, the Internet may serve as an additional source of evidence that a crime has been committed such as through browsing history, chat conversations, bank transfers, or evidence of contact and communications with other offenders. Digital evidence can now be gathered through cell phones, laptop computers, cameras and other technology devices. This technical evidence allows for more successful criminal prosecutions.

**Methodology**

This study consisted of a thorough review of available scholarly research with focus on recent literature published within the last three years. Since technology changes rapidly, it is important to focus on current research that is aimed at the evolving realm of cyber crime. For this reason, special attention was paid to scholarly research articles published from 2011 on.

**Summary, Conclusions, and Recommendations**

The Internet has drastically changed business, education, and the economy. The Internet has grown much quicker than anyone ever imagined, and as such, law enforcement and the judicial system have struggled to keep up. As technology has progressed worldwide, the complexity of the crimes has also grown significantly. Cyber systems run nearly all critical infrastructures in the United States and are the backbone of America’s national security and economic success. This critical infrastructure is more digitally interconnected than ever. The advancement of technology and, most importantly, the Internet has provided offenders and organizations with a means to commit new types of crimes and adopt new methods of committing traditional crimes such as theft and other property crimes. With the use of the Internet for commercial purpose, the method of perpetration of fraudulent activities has evolved
to include online capabilities. While the Internet has revolutionized nearly every aspect of daily living, it has also created a wealth of new opportunities for crime. Millions of people are now affected by online criminal behavior. As the Internet continues to expand and more people have online access, there is no doubt that terrorist groups and other criminals will continue to exploit the Internet for all aspects of their operations. There is widespread agreement among governments and lawmakers that the Internet creates serious opportunities for criminal activity and that action is needed to counter this growing threat.

It would be nearly impossible to completely eliminate cyber crime; however, it can be minimized. Since it is unrealistic to “pull the plug,” steps must be taken to mitigate the threat. The challenge lies in managing risk so as to achieve the maximum benefits which flow from new technologies, while minimizing the looming threat of cyber crime (Grabosky, 2000). Collaborative efforts must take place between individuals, corporate organizations, industry and law enforcement agencies, and the government. Victims of cyber crime need to become aware of such crimes and they need to become more educated in how to protect and prevent not only themselves but others as well from such malicious acts (Kamal et al., 2012). Youth should be educated, perhaps through youth training centers or as part of a mandated social and law studies class, to understand the adverse effects of piracy and other Internet crimes. Organizations and learning institutions, such as universities and colleges, should engage their system administrators and IT personnel in annual training to better understand emerging technologies in the market. Current training equips technology and computer professionals with the necessary skills to be ready to combat cyber crimes. With regards to child pornography, training for law enforcement and other professionals needs to address the evidential issues relating to the pictures and videos, with special emphasis on tracing the chain of postings to the original producer. To understand the
processes involved requires knowledge of the behavior of the producers and downloaders and the language they use to communicate.

To successfully stop child pornography and abuse, there should be legislation for the mandatory reporting of child pornography. This would inevitably raise concerns about censorship and privacy, but the proliferation of this crime must be stopped. Protocols should be established with regards to countries who continue to facilitate the production and distribution of images portraying the sexual abuse of children. Strict global penalties must be enacted for those who continue to produce, distribute and view child pornography.

There remain many challenges for law enforcement agencies in relation to cyber crime and, specifically, cyber terrorism. Terrorist use of the Internet is a transnational problem, requiring an integrated response across borders and among national criminal justice systems. Many cyber crimes originate in one country but are initiated by attacking units in different territories which makes tracking the perpetrators even more difficult. Many countries lack the technical capabilities to investigate online criminal activity, especially the organized activity of a technologically advanced terrorist group. Developed countries must assist small and poorer nations that lack the resources necessary to investigate cyber crimes. Developed nations should provide assistance to these countries, especially those that have high rates of origin of cyber crimes. This is one of the few ways to combat global cyber threats that originate from these countries (Kshetri, 2005).

It is evident that existing international conventions are not effective in prosecuting and combating cyber terrorism. It is vital that an international legal framework is created to meet the challenges posed by cyber terrorism. Even after an international legal framework is established, the even greater challenges will lie in policing and detection of cyber crimes by law enforcement
officials. Governments, especially of countries were cyber crime laws are minimal, must assure that their laws and new legislation apply to cyber crimes. Although some government agencies around the world have taken precautions to detect and prosecute perpetrators of cyber crime, enough action has not been taken to effectively deter criminals from committing illegal acts. There is a definite limit to what one country can accomplish on its own. If the United States continues its crackdown on Internet crime, perpetrators can easily relocate to other jurisdictions that are less vigilant about monitoring and countering illegal online activity. Nations around the world are tasked with forging policies on where to draw the line on such fundamental questions as the balance between a citizen's right to privacy and the sworn duties of law enforcement. Because of the vast amounts of new technology being produced regularly, government agencies must stay alert and informed in order to control cyber crime.

Unfortunately most organizations and individuals adopt a reactive rather than proactive approach to information security. The vulnerability of a system is usually evaluated after an attack takes place, resulting in money spent on fixing the security holes and recovering from the data and business loss. This the most expensive and least effective approach. One of the easiest ways to protect from unethical data loss is physical data security. All confidential information should be securely locked away from unauthorized users. Technology users should be educated about potential threats and learn how to keep themselves and their family members safe from cyber criminals. Special attention should be paid to young people. Children must be shown how to use the Internet safely and responsibly.

Technology changes constantly, and to be effective in combating cyber crime, industry and enforcement agencies must increase and improve their understanding of available technology and how deviants use these sophisticated means to commit crimes. As technology has
progressed, computer crimes have become more complicated. Enforcement agencies must understand the legal process and requirements for evidence collection and presentation in judicial process of these unique crimes. It is not only enforcement and industry professionals that should receive specialized training. With the increased use of the Internet, individuals need to be fully trained on the threats they face as a technology user. There is an urgent need for information security, ethical education, and awareness programs to inhibit the proliferation of cyber crime.

The Internet has brought to light issues with trans-national crime and the ability to successfully prosecute these crimes. Cyberspace is not the first or only policy domain which lies beyond the control of any single nation. These issues have been confronted in the past with international air traffic, funds transfer, and environmental considerations, to name a few. The development of international arrangements has been necessary and will continue to be so as global connectivity continues to increase. It is important for governments and law enforcement personnel to be one step ahead of criminals in terms of the use of technology in order to prevent or counter unlawful online activity. Professionals must understand the impact of technology instead of only focusing on the technology itself.

The Internet has created a world where educators, parents and lawmakers fear they cannot keep up with the rapid shifts in technology. Legislation is slowly growing to accommodate the technology age. As social networking sites continue to develop and expand and communication advances in other countries, it is imperative to stay vigilant to safeguard against cyber bullying and online harassment. New laws are increasingly requiring schools to adopt policies on cyber-bullying and online harassment and consequences for ignoring the impact of this environment on school bullying policy can result in legal problems when they occur (Jones et al., 2013). Online harassment is an area that clearly needs more research to
understand the most distressing kinds of harassment and the aftermath of online harassment episodes. There is also a need to understand and measure the positive, not just the negative, aspects of online communication with peers, family and friends. It is important that education programs to address cyber bullying and online harassment be evidence-based and thoroughly tested prior to implementation rather than a knee-jerk reaction to appease lawmakers and the public.

Research on cyber crime data is minimal in comparison to traditional crime, the main reasons being cyber crime is a much newer concept and the limitations of available data. Research and its subsequent results are limited to the quality of the available data which means the advancements in cyber crime data must be a priority. Standardizing data and reporting measures will increase available information on cyber crime and build reliability and validity of the data. Studies should be done to compare the characteristics of online and offline offenders to establish if these groups of perpetrators are different. The results of these types of studies will help shape policy and intervention strategies. Research in this field must continue to better understand cyber criminals and, more importantly, laws must be enacted to ensure successful prosecution of these criminals.

Internet users must learn to protect themselves and their families from the dangers of Internet based crimes, such as cyber stalking and identity theft. It is apparent that anyone, including man, woman or child can become a victim of an Internet based crime. With the increasing availability, use and reliance on electronic technology, the issues outlined in this paper are going to become more important and are clearly worthy of greater study and understanding. There is a clear need for further in-depth research in understanding and addressing the multiple issues and consequences of cyber crimes nationally and globally. It is important to study the
effects of the Internet and cyber technologies on all aspects of life including commerce and education. Cyber crime and cyber victimization will continue to be growing areas of research and policy influence as the world grows increasingly reliant on cyber technologies and the Internet.
References


http://dx.doi.org/10.1007/s10611-007-9059-3


http://dx.doi.org/10.1080/15614263.2011.62746


Muthama, M. N. (2013, August 31). Regulation on access to Internet: Problems and solutions. 


http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat


