International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Impact of Cybercrime on Youth in India

Ghone Siddhesh Jaywant

Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

ABSTRACT

Cybercrime will have a big impact on young people. Young adults are more likely than any other age group to gain access to the Internet because they are the first victims of cybercrime. This article would look at how cyber-crime affects and creates challenges for the younger generations. Topics such as fitness, especially emotional well-being, are devoted to explaining many cybercrime issues. Many young people have attempted to kill themselves because they have become victims of cybercrime. This document would look at all the consequences of cybercrime, including cyberbullying (a type of cybercrime), and how young people can prevent cybercrime.

KEYWORDS: Cybercrime, Young adults, Cyberbullying, Advanced Technology, Internet

I. INTRODUCTION

Cybercrime is a term used to broadly define illegal activities where machines or computer networks are the weapon, the destination, or the scene of the crime. It also includes typical crimes that use machines or networks to enable criminal behaviour. Cybercrime will stop any train it's on, mislead planes in flight, get any valuable military data into foreign hands, stop email, and cause any device to fail in a fraction of a second. This thesis deals with the many dimensions, effects and perspectives of cyber technologies with special reference to cyber-crime threats from India. A review of the legal system applicable to its regulation in India has been undertaken. To begin, the measures of "crime" must be defined. There is also no doubt that "crime" is a relative term that is common in nature and has clearly demonstrated its existence in all cultures, from ancient to modern. Each society provided its own definition of illegal behaviour, punished by the express will of the political community to rule the society, which was often influenced by the economic interests of the religio-socio-political society. So the behaviour that was often conditioned and marked by the ultimate consequence of these criteria was "criminal liability". Parenthetically, as the definition of crime has changed, the types of offenders committing these crimes have changed with the advent of information technology. The concept of crime marked by religious understanding is relevant to Indian culture, especially in ancient times. The era was famous for the full reign of faith. The intervention of a supernatural force found that both political and social events in general and "crime" in particular had taken place. This time it arose from the demonological theory of crime. The Middle Ages showed times of revival and renewal that gave "crime" a modern appearance. Concepts such as utilitarian method, constructive approach, analysis, ideals of natural justice or ideas of laissez faire, hedonistic ideology and the idea of pain and pleasure became the result of the era that helped to open wider horizons of crime research. The later era paved the way for revolutions in science and industry, and logical interpretation influenced thought. Computer technology services were not without inconvenience. And if it makes life too fast and fast, it almost ceases to function in covering threats from a deadly type of crime known as "cybercrime" without computers. The abundance of cheap, powerful and user-friendly computers has allowed more and more people to use them as part of their daily lifestyle. Perpetrators continue to depend more and more on them as companies, government departments and individuals. Cybercrimes are limited until their behavior and impact on different levels of society, especially young people, are properly analyzed and understood. In collaboration with the US Federal Law Enforcement Agency, International Computer Crime Squad [CSI/FBI 2006], the Computer Security Institute's 2006 Computer Crime and Security Survey found an alarmingly high number of companies experiencing problems with electronic and Internet fraud. Of the companies that acknowledged financial damage from the computer breach, several failed to estimate the losses. Machine Vireo observed 65%; 48%, in one to five security events, recorded between one and five; Incidents from sources within the organization were identified by 42%; In the past year, 32 percent of respondents used their operating systems incorrectly; Laptops and handheld devices were stolen by 47 percent; in e-commerce: Both participants had some kind of website incident: 9% said confidential data was stolen; 6% reported site defaults; 9% were financially fraudulent. Sabotage was 3 percent. Data protection losses totaled more than $52 million in 2006, down 30 percent from $141 million in 2004. However, these numbers refer only to the 313 respondents who advised the CSI/FBI survey results and not to all US firms. Worth mentioning. It was sent out in response to 5,000 businesses in January 2006 with a 6% return.

II. CATEGORY OF COMPUTER CRIME

For intelligence gathering, cybercrime and data capture purposes, while the connected one monitors data flows to or from the destination. This attack may be carried out to gain intelligence for the benefit of a future attack, or the collected evidence may be the ultimate goal of the attack. In general, this attack involves the monitoring of network traffic, however, some data sources, including the radio, may be observed. In most types of attacks, the attacker is passive and only monitors the correspondence regularly, but in certain versions he may try to set the data flow or manipulate the nature of the data being transmitted. However, the intruder is not the intended recipient of the data source in all versions of this attack, distinguishing this attack from other types of data collection. The intruder not only observes the obvious data sources (eg networks) and reads the content, but also several other data leakage attacks. This is not the same as attacks that collect more qualitative details, such as the number of contacts, that are not explicitly transmitted through the data source.

Data Modification

Communication privacy is essential if data cannot be changed or accessed in transit.

A distributed environment allows a malicious third party to commit cyber fraud by manipulating data as it travels across locations. A malicious entity in the network captures and modifies portions of the data before retransmitting the data in a data manipulation attack. The value of a financial transaction from $100 to $10,000 has changed from one image. A whole series of valid data was often injected into the network during a repeated attack. One example was to replicate a legitimate $100 bank payment transaction thousands of times.

Data Theft

Terms used to characterize an unauthorized copy or removal of knowledge by a company or other person. In this regard, user data such as codes, social security numbers, payment card details, contact records or other private organizational information are often used. Due to the illegal collection of this material, it is likely that the person who stole this information is apprehended to the fullest extent of the law.

Cyber-Crime and Cyber Interference

Network Interfere with the functionality of a computer network by entering, transmitting, damaging, erasing, impairing, altering or erasing network data.

Network Sabotage

"Network sabotage" or inept admins who are usually responsible for individual tasks. The above can be a single item or a combination of items. However, if Verizon uses a child's device to prevent first responders, it could raise the network's concerns to prompt the federal government to intervene for public safety purposes. If the federal government is obliging these citizens to do what the unions intend to do and go on strike, that is obvious.

Criminal Access and Unauthorized Access

An inside look at the underground cracker machine is "Unauthorized access." The films were shot in the USA, Holland and Germany. "Unauthorized Access" explores the characters behind the computer screens and tries to distinguish the media hype of "outlaw hackers" from the truth.

Spreading Viruses

Malicious software that attaches to other software. (Victims' systems are destroyed by viruses, worms, trojans, time bombs, logic bombs, rabbits, and bacteria).[1]

Related offenses such as aiding and abetting cyber crimes

There are three factors in most charges against a person. First, the crime was committed by another person. Second, the accused person was aware of the crime or the motive of the principal. Third, the individual supported the principal with some support. An accessory is usually identified as a natural person who assists another person or others in the commission of a crime. In some cases, the person responsible for aiding or abetting the crime is aware of it before or after it is committed. An individual who is aware of the crime before him and who provides some kind of assistance to those who commit it is legally recognized as an "accessory". It can help with leadership, actions or financial assistance. An individual who is innocent of a crime but who assists in the commission of a crime is called an "accessory"[2,3].

Computer-related counterfeiting and fraud

Computer forgery and computer fraud are computer-related crimes.

Content related crimes

Content-related offenses include cybersex, unwanted commercial contact, cyberslander and cyberattacks. The estimated cost of the victims of these attacks is 1 trillion dollars per year, which is a substantial improvement for developing countries in the situation of non-German or underdeveloped countries. Details provided by America's primary news agency are necessary for certain cybercrime facts:[4]

1. Studies have also shown that in the past two years, one in five Internet shoppers in the United States has been a victim of cyber fraud.
2. EMC's protection division, RSA, released Q4 analysis on identity fraud, phishing and ransomware, privacy breaches and data shortages.

i. The review found that 23% of the global population would be spear-phished, while the average website will be compromised every 4.5 seconds.

ii. Cybercrime costs businesses in Australia more than $600 million a year, while the cost of cybercrime in the US has fallen to one in five internet users, or $8 billion, over the past 2 years.

iii. The review also showed that online user protection is even more of a concern. A 2009 US consumer awareness survey found that 85% of respondents expressed concern about the security of data transmission over the Internet, while 59% expressed a desire to increase data privacy on their websites.

iv. Between 2004 and 2007, there was a 50-fold increase in spam, hacking and fraud.[5]

3. According to a recent survey, in 2008 India became the fourteenth country in the world to host phishing websites. Moreover, the boom in call centers in India has created a space for cyber-crime in data collection.
4. Prasun Sonwalkar's words represent India's cybercrime challenge — India is fast becoming a global hub for cybercrime as a slowdown turns casual criminals into electronic fraud, according to a report by Brighton University academics. The report, titled "Crime Online: Cybercrime and Illicit Innovation", says that cybercrime is a source of "particular concern" in India, China, Russia and Brazil, and that the large number of call centers is the cause of "the breakthrough in cybercrime in India in recent years. At the scene of the crime in the UK, the association representing police officers was provoked in the FT to claim that "the police remain in the background of sophisticated gangs", that the value of online theft in the world is about £50 billion a year. Computer spam refers to unwanted Internet promotional advertising that can often transmit viruses and other programs to computers. So far, the UAB Spam Data Mine has analyzed millions of spam e-mail messages and effectively linked thousands of advertised websites to 69,117 separate spam hosting domains, Warner said. Warner. Of the total number of domains analyzed, 48,552 (70%) had internet domains – or addresses – ending in the Chinese country code ".cn". Additionally, 48,331 (70%) sites were hosted on Chinese machines. In India, the main identified cyber-crimes are denial of service, website defacement, SPAM, computer viruses and worms, pornography, cyber hyper infection and cyber stalking. With around $120 million worth of mobile telecommunications lost or stolen worldwide last year, consumers must encrypt documents, contact information and phone numbers to prevent them from being misused. Current and former employees and hackers carry out nearly 69% of intelligence theft. India has to spend a lot of money to secure sensitive records. In its first comprehensive survey on the Indian Net Scene, Symantec shares the numbers: The country ranks highest in the world (76%) in legitimate email traffic with outbound spam or junk mail. Home computer owners in India are the most targeted sector of India's 37.7 million Internet users: More than 86 percent of all attacks, primarily by bots, targeted lay surfers, with the two most vulnerable cities being Mumbai and Delhi. Many countries in Africa neglect cyber policies and legislation (many articles and reports are available on this support). Because of this and that, the cyberterrorist escapes. Cyber rules and regulations are almost free in countries like Kenya, Nigeria, Tunisia and Tanzania etc. The above text covers only a few cases of the dire state of cyber-crime in India, USA, Europe, Asia and Africa.

III. TYPES OF COMPUTER CRIME

Theft of telecommunications services Theft Three decades earlier, the "telephone phreaker" provided a precedent for a major criminal sector. Through PBX access, people or illegal groups can gain access to dial-up/outgoing circuits and either make their own calls or offer call time to third parties (Gold 1999). Criminals can gain access to the control panel by impersonating a technician, fraudulently obtaining an employee's access code, or using software on the Internet. All advanced criminals loop between PBX networks to avoid detection. Additional Services provide collection of "calling card" information and sales calls paid to calling card accounts, including counterfeiting or illegal reprogramming of stored value calling cards. Offender Support Communications The operations of criminal organizations are technologically enhanced, just as legitimate private and public organizations rely on information systems for messaging and record keeping. Telecommunications facilities have been used to support systematic drug trafficking, gambling, prostitution, money laundering, child pornography, and arms trafficking (in those jurisdictions where such activities are illegal). Criminal messages can be kept out of the control of law enforcement agencies using encryption technologies. Increasing emphasis is being placed on the use of computer systems to create and transmit child pornography. These goods are now available for import at a light pace across national borders (Grant, David, and Grabosky 1997). Some of the more obvious forms of Internet child pornography involve a moderate degree of coordination, as required by the IRC and WWW infrastructures. Piracy in telecommunications Digital technology facilitates the reproduction and distribution of paper, audio and multimedia variations. Many people have proven irresistible in their attempt to replicate the copyright for personal use, to sell at a lower price, or even for free delivery. The creators of proprietary works made a point of it. Copyright infringement is estimated to cost the market between $15 billion and $17 billion annually (United States, Information Infrastructure Task Force 1995, 131). If the designers of a particular work are unwilling to take advantage of his inventions, this can usually have a refreshing effect on the artistic endeavour, in addition to financial failure. Dissemination of offensive material Content in cyberspace is often considered unacceptable by others. It contains, among other things, sexually explicit content, racial advertising, and instructions for making fire and explosives. Telecommunication mechanisms can also be used to intimidate, threaten or disrupt correspondence from conventional obscene telephone calls to their contemporary manifestations of "cyber chat". Electronic money laundering and tax evasion For several years, electronic money flows have helped to hide and move the proceeds of crime. Emerging technologies can profoundly help disguise the source of unattainable profits. Legally generated income from the tax authorities can even be more easily hidden. The only financial entities capable of achieving electronic funds transactions that traverse multiple jurisdictions at the speed of light would undoubtedly be the larger financial institutions. The creation of informal banks and parallel banking structures will make it possible to overcome the regulation of central banks, but also help prevent the reporting of cash transactions in countries with them. The use of telecommunications will create the traditional underground banks that have flourished in Asian countries for decades. Vandalism, Terrorism and Electronic Extinction Western industrial civilization relies more than ever on sophisticated data processing and telecommunications networks. Damage to or interaction with any of these structures can have catastrophic consequences. If driven by fascination or justification, technological interlopers are at best an inconvenience and can cause enormous damage.[6]

Sales And Investment Scams

The widespread use of new technologies for illegal endeavors would be even greater as electronic commerce grows. The use of telephones is increasingly prevalent in false advertising promotions, fraudulent charity solicitations or deceptive investment opportunities. Cyberspace now offers many investment options, from conventional stocks and shares to exotic opportunities including coconut farming, sales and leasebacks on vending machines and international telephone networks. In fact, modern times have seen unprecedented disinformation opportunities. Fraudsters already have immediate and limited ties to millions of potential victims around the world.

Illegal Wiretapping Of Telecommunications

New possibilities for electronic interception are emerging in telecommunications. Telecommunication eavesdropping is increasingly applicable, from the best practices of spying on an unfaithful partner to the latest methods of political and industrial espionage. Again, new vulnerabilities result from technical progress. Another possibility is to capture the electromagnetic signals generated by the robot. Cables can serve as antennas for broadcasting. Current legislation would not prohibit remote control of computer radiation.

Electronic Money Transfer Fraud

Electronic fund transfer networks have begun to proliferate, creating the risk of interception and diversion of such transfers. Valid payment card numbers can be intercepted both remotely and physically; the data stored on the card can be falsified. Just as an army thief can hijack a motor vehicle for a quick getaway, so telephone systems can be hacked and used for vandalism, bribery, or the promotion of a criminal conspiracy. In the context of cybercrime, two or more of these general types are combined.

IV. IMPACT OF CYBER CRIME

Crime as a bad social factor Because a crime-free culture is an illusion, crime is a pervasive phenomenon and an inseparable element in social life, the question "Why is there so much crime uproar?" is irritating. Crime, as one of the characteristic features of any society, whether civilized or undeveloped, and one of the basic impulses of human behavior, is nothing new. It is omnivilized, ubiquitous, and there is nothing new about crime. However, social anxiety about high crime should be considered not because of its origin, but because of the potential disorders it causes society. In addition, several people are specifically victims of violence. Anything meaningful can be lost to the survivor. Security, harmony, money and possessions can be essential virtues because they can satisfy several desires. Impact of cybercrime on social and environmental policies Crime is a complex and relative phenomenon conceptually and is subject to relative sociopolitical and economic shifts in contemporary social systems. As a result, no systematic understanding of all forms of "crime" is available in a given period and cannot be applied to a single definition in any culture. It is influenced by the variations of related phenomena and the value framework generated by these shifts with their dynamics. A definite increase in corruption-based crimes, where there is little social moralizing and the commission of crime is undermined by less social shame, is taken for granted in today's situation where money is more important than ideals. However, economic crime is at its peak. This directly shows that crime is interdependent on other social phenomena, economic processes and political machines. Demographics are also one of the main variables that influence the impact of crime. A strong correlation was found between the increase in the incidence of crime and the population of the region. Other variables that determine crime include the situation in a particular locality, the degree of urbanization, demographic displacement from surrounding countries, housing, economic differences, [technological literacy in the field of cybercrime], etc. 2 At about the same time, economic crimes are also affected by the social donation system. Because every crime prevention scheme has something to do with the political system prescribing norms, making laws, creating protective measures, the political process and mechanism affects crime in a particular community. This clearly shows that the concept of crime is related to socio-economic and political conditions. The impact of cybercrime on young people Cyberbullying is the biggest fear in the minds of young people today. It has been widespread in the last five years, mostly from the age of under 18, and cyberbullying is the most sensitive and feared inspection. This is becoming a disturbing pattern in our culture. Young women have the worst fear of cybercrime, according to the results check. Cyberbullying is the fear of being attacked, negativity or derogatory photos or comments of another person. This is primarily achieved through the key online technology mentioned above. You can chat, text, etc. Cyber Bullying.

Where websites like Facebook, Orkut, Twitter consumer is most affected. My research shows that an individual who is routinely hated will reach a ceiling of depression, embarrassment, and threats. This research makes it possible to analyze whether Bulled will be stressed to the point of self-harm, whether he is online. The Impact of Cybercrime on the Private Sector I could use the terms invasive, silent, and risky if I had three characteristics to characterize cybercrime. The very silence of this type of crime is a great challenge in the fight against danger. In fact, very often businesses forget that they have suffered a fraud or attack until long after the incident. The effects are disarming, as it is often difficult to find a case again, just as the time gap between the crime and its discovery offers advantages to those who commit crimes that are sometimes insurmountable and make prosecution impossible. But the truth is that many businesses have actually been victims of cybercrime over the years, but are unaware of the cancer that is destroying them from within. It is not so. But that's true. The Ponemon Institute's second annual Cost of Cybercrime Survey, released by the Ponemon Institute, shows that while a greater understanding of the cyber threat has significant financial implications for businesses and government entities, the study focuses on a representative sample of 50 larger organizations. The research is published in the Ponemon Institute. The study reveals that the average annual cost of cybercrime to 50 organizations is $5.9 million per year, ranging from $1.5 million per business to $36.5 million per year. Compared to the first report in the previous year, gross costs are higher.

The Impact of Cybercrime on Youth

The newest way of communication is the cybernetic. Online social networking blogs, instant messaging, and email provide consumers with an easy and fast way to communicate with others around the world. Teenagers spend hours online every day, especially on computers or electronic devices. Family-rescource.com reports that 48% of teenagers agree that the Internet strengthens their friendships. Thanks to the popularity of social networking platforms, young people can keep in touch with real friends online. Some young people say that cyber interactions allow them to feel confident that they are their true selves. Used by approximately 13 million teenagers, instant messaging programs facilitate real-time discussions with peers. The way to partner with other teens is open near and far with online networking platforms. Writing when teenagers are mostly online has no structured cyber communication writing skills. On the contrary, young people often write digitally in jargon, abbreviations, or slang. The National Commission on Writing reports that 85% of teens use social media to communicate, but 60% do not see the form of communication as "writing." Teens should consider the difference between formal and informal writing and understand whether it is appropriate (in school).

Cyberbullying

Online contact among young people has a negative impact on cyberbullying. Victims of cyberbullying also face social media rumors and misinformation online. Bullying images of their victims may seem indecent or shameful. Another aspect of cyberbullying is the use of rude text messages as harassment. The National Crime Prevention Council reports that more than half of American youth have experienced online bullying. Young people have taken their own lives due to online bullying in some serious situations.

Sexual Harassment

For teenagers who use forms of cyber communication, sexual harassment is an increasing concern. This can happen on social media platforms or chat rooms. Sexual application occurs whenever an adult or friend attempts to have sex online. A teen may be asked to share personal information, watch porn, or talk about sex online. About 70 percent of teenagers online are female. Young people should be careful about posting provocative pictures and talking to strangers in online chat rooms.

V. FUTURE TRENDS IN CYBER CRIME

One of the more alarming phenomena is the rate of increase in cybercrime. "Last year was the first year that cybercrime revenue was greater than revenue from illegal narcotics sales, and I think it's more than $105 billion," says Valerie McNiven, an American financial advisor. She said that more "In such fast cyber crime is on the move that the police can't catch it. It is certain that the problem can only get worse in the coming years as professionals have noticed the windfalls if used correctly. There has been a lot of discussion lately about organized crime and cybercrime mergers. Such a connection foreshadows an unpleasant smell in the foreseeable future. With several criminal gangs from Eastern Europe, Russia and Asia, with little legislation and enforcement, there is little hope that conventional means can contain and neutralize the danger. Phil Williams, visiting researcher at CERT, summarized the problem succinctly. "The Internet offers all the criminal networks and targets and can be used with very little risk for significant profits. It's hard to ask for more for organized crime." As a result, an increase in advanced phishing attacks and other means of two-way identity fraud can be anticipated. For example, call centers can be used to alert consumers in advance of a problem and then follow up with emails that request personal information. In several third-party data centers, the addition of personal data can prove useful targets for infiltration. It's not hard to imagine criminals using data mining technology to find the most vulgar customers or to tailor phishing emails to real individuals based on their health, financial or personal background. Theft can now be identified in more automated ways. For example, a botnet can be used to find personal information such as credit card information and social security numbers, not just for denial of service and spam attacks. Botnet administrators may accept compensation for their "database" requests. It begins to ask where all the technological know-how to carry out cybercrime can come from for the sophisticated criminals who run the money laundering and organization of these systems. Unfortunately, there is an increasing number of smart all-university blackhats, often working in countries where legal work is scarce and the risk of getting caught is small. However, being a hacker willing to do a lot of damage to networks and carry out cybercrime is more worrying than ever. The Internet has provided a knowledge base where anyone can learn the basics of subverting computer systems, and several videos available that explain to the near-layman how to perform a buffer overflow or man-in-the-middle attack. It is interesting because those who do not take the initiative to study and discover new achievements are not the main challenge. This community is likely to remain a small, very smart network of researchers and conservation organizations that focus exclusively on software issues. This requires a certain amount of investigation, expertise, and persistence that most are unable to expend, even if one is inspired to understand how exploits work. The real threat comes from the sheer ease with which someone can run a program like "MetaSploit," a system that allows new modules to be downloaded and run instantly. Apart from how humans operate, the perpetrator simply has little to do with machines. In fact, almost all attacks are diligently worked on by a small number of individuals and eventually released into the public domain, allowing virtually anyone to perform an attack. Botnets are no longer hand-crafted applications by a single party that has truly understood their fundamental principles, but instead open-source community projects that ensure distributed computing like BotNET, Eggheads, and CSharpBot, all available from Source Forge, can be controlled as easily as possible. . The barrier to entry into the sector is so minimal that almost anyone will experiment and enter cybercriminals. Since the learning curve is too short, there should be a quick discussion about how to prevent and deal with offenders in a way that is no longer tied to outdated approaches. For example, once someone enters a house, they must prepare not only for the right time, but also to beware of picking locks, escaping the protective framework, and the abyss of crossing moral thresholds. In contrast, the ease of cybercrime appears inversely proportional to its profitability, and moreover, these patterns show signs of acceleration.

VI. CONCLUSION

The future of the Internet remains for predators and ordinary people. There are also many fears of a cyber apocalypse, with the potential damage from large-scale fraud almost limitless. These concerns should be reasonable, knowing that problems are being addressed, but not quickly enough. The value of the internet has been shown in many ways that I believe would be enough to keep it from becoming a wasteland of crime and a bastion of bad people. The government also has an important role, but private companies that produce apps and others that are able to deter fraud must do a lot of protection. Consumer services only concern a minority of potential victims. Others must be immediately covered by steps that are not stressful and require significant involvement. If it works, security needs to be simple and effective. There's no telling if cybercrime will be a relevant issue ten years from now, so as the internet continues to grow, it needs to be addressed so that the reality of cybercrime is commensurate with real crime, if not greater. The role and contribution of parents and teachers is essential to monitor and prevent the impact of cybercrime on young people so that they can make better use of them without being held back by incompetence and unregulated behaviour.

REFERENCE

1. DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-

2. IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/,

3. Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012

4. Legal Info (2009), Crime Overview aiding and abetting or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

5. Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/forensic/cybercrime.htm,

6. Hundley and Anderson 1995, Schwartau 1994