What is cyber crime media essay

Media

From Fiction to RealityAlexandra AbalaseiVisual CultureProfessor Cristian PraleaFebruary 12, 2013

What is Cyber Crime?

In the last fifteen years, millions of various websites have been created, allowing people the opportunity to do business, play, study and communicate online. Today, it became easier and cheaper to do all these things. The beginning of the internet has immeasurably changed the manner in which people access or look for information. News broadcast moves more rapidly than ever, and all gossips, affairs, even political things can be discussed via e-mails, blogs or social networks (Facebook, Skype, My Space and so forth. Many people argue that the Internet is controlling the lives of its users and it is harmful, while others enjoy of increased number of opportunities, and the way they keep in touch with friends, loved ones, colleagues. A few would deny that the Internet has a considerable impact upon criminal behavior. Even if this rapid development of Internet has a tremendously influence on people’s lives and many take advantage of its benefits, it also allowed a great amount of insulting, discriminatory, illegal information that can be easily accessed. Persons who are more vulnerable could be easily exploited if discovering that kind of information. The purpose of this project is to contribute to our knowledge and understanding of cyber crimes. Also, to illustrate and exemplify the types of crimes that occur behind the screens, further, focusing on how terrorist acts became real after their initiators have gotten their inspiration and information from the Internet. Cyber Crime, computer crime or electronic crime is usually defined as any sort of illicit activity, where the Internet or a computer is the tool,

cause or target of a crime. Furthermore, even though these terms are more accurately limited to describing immoral activity in which the processor or network is an essential component of the crime, they are also from time to time used to involve traditional crimes, conducted through the Internet. For example: fraud, robbery, blackmail, falsification, credit card accounts theft, pornography and pedophilia, in which computers or devices are used to facilitate the illicit activity. The term " cyberspace" was made up by William Gibson[1]in 1982, and in his novel " Neuromancer" (1984), the term became popular, describing the psychologically built virtual environment, in with networked computer activity takes place. " Cybercrime" is referring to the crimes that take place within that particular space and signify the risk and insecurity online. The beginning of those crimes lied in some unsatisfied employees' acts, which caused a tangible damage to the computers they worked with, in order to get back at their supervisors. The facility to have individual computer at home, became easy to get to and very popular, thus, cyber criminals paid attention to the home users. The crimes which were frequent during those times were phishing, viruses, identity theft or harassment. Cyber Crime turned out to be larger and harder to control as the years went by and more and more families bought home computers with Internet access. Today's technology has made cyber-crimes even easily to commit, because criminals do not have to expose their faces on the Internet. Moreover, in modern days, the economy is very poor and unemployment rate is higher; individuals are struggling to obtain a good job and it is quite miserable the fact that criminals try to take advantage of them by sending through e-mails regarding job offers to trick those into falling for payment transfer scams.

A Brief Classification

Network safety has become a major concern through the years because, once with Internet’s growth, cyber crimes emerged rapidly. The usage of information technology has become advantageous, but in the same time, insecure. Stealing money, intellectual property, hacking into someone’s computer, sexual harassment – those are few examples. There are three important types of cyber crimes: the crimes against the person, property and the government. In this category (cyber crimes against the person) is included harassment, a crime known as " cyber stalking’. This type of crime represents a real social problem that is speedily increasing. Cyber stalking is a crime in which the harasser uses electronic communication or mediums of Internet (instant messages, e-mail, cell phones or chat rooms) in order to threaten, sexually or emotionally harass, even to misinform the victim. The messages must be unsolicited and usually, those actions take place over a long period of time. The aim of those messages is to create fear for their victim." The fact that cyber stalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyber stalking."[2]According to Maxwell[3](2001), most of the victims are regular people rather than popular and rich, moreover, they are females, with age between 18 and 30. Stalking as a crime not in favor of young people may report for the prominent occurrence of cyber stalking

victims inside universities (for example, the University of Cincinnati study showed, 25% of college women had been cyber stalked). The second category is stalking against the property, which includes crimes such as computer vandalism, transmission of harmful programs and destruction of other’s property through Internet. A significant example of such crime would be hacking. Hacking or Cracking is a widespread cyber crime committed nowadays. Hacker[4]is " a term for both those who write a code and those who exploit it". Hackers make use of the vulnerability of victims’ computers to steal important information and destroy data. A cracker is a hacker with criminal intention; he can sabotage or damage computers, steal information located on locked computers, and cause disruption to the networks for personal or political motives.[5]Hackers can install programs on victim’s systems without their knowledge, stealing personal or credit card information, passwords and so on. They can also hack important data of companies, in order to get secret information about their future plans. One of the most grave cases of hacking took place in Canada, February 2000, where a juvenile (known as " mafiaboy"), pled guilty to 56 charges for illegal use of computer service. Sites like Yahoo!, CNN, eBay, Amazon, Buy. com were taken down by DDoS[6]attacks.[7]The most serious cyber crime in this category is the crime against government. Because the society became so dependent on Internet and computer systems, the threat of cyber terrorism and the exploitation of the Internet for terrorist objectives are quite troubling. This danger is not about to be neither denied nor unnoticed. The Internet is perhaps not a substitute for face-to-face communication, but, in a world where the personality rises above politics, individuals are no longer used to doing things together or performing public roles; for that reason,

they are not capable to find society and the confidence (privacy) it gives. According to David Wall, globalization has created crime opportunities across cultures and authority by enlarging the reach of criminals at a global level. As a consequence, globalized information made criminals' imagination wider, cyber crimes being, then, a globalized phenomenon. Since Internet and the abuse of information became so available, not only experts but also terrorist organizations take advantage of gathered information. Normally, a terrorist takes a long time perspective; to accomplish his objects, he pursues a fundamental schedule when committing attacks. Furthermore, there are three main objects identified in a terrorist view: causing an economic disorder, discriminating the adversary, the generation of financial income for the terrorist organization. The first two objects are related to each other, both trying to show the deficiency of technological information and the vulnerability of state security and industry. Successful attacks manage to create panic, public danger or intimidate, demonstrating attacker's terrorist competences. There can be distinguished four different types of attacks that appear to be interesting for terrorists: large scale attacks, hacking attacks, hybrid attacks and attacks resulting in physical damage.[8]Attacks are launched via Internet, thus, they use network to communicate with the public or with each other. This fact is quite important because is it the way to explain the motivations and causes for terrorists' battle, to recruit new members and train them or to distribute pressure and misinformation. In addition, the access to systems that control IT-infrastructure can be abused to cause physical harm, the attacks prevailing on military productions, transport areas and energy services. Therefore, it could be considered a " pay off' for the human lives affected, if an amount of money, knowledge and

time were invested in the terrorist organization. In conclusion, I would state that Internet is constantly having a tremendous impact for criminal activity and behavior. An essential question arises that how can these crimes be banned. Even though many solutions have been presented namely: ant viruses, firewalls, cryptography and cyber ethics and laws, the problems still exist and they are increasing day by day, as long as the amount of information becomes more and more available and new technologies continue to develop.