ISBN: 978-93-92995-10-1

CYBER CRIME AND NEED OF CYBER CAMANDOS

SHIVAM KUMAR SINGH
Email ID: shivamkumar.singh2018@vitstudent.ac.in

Abstract
In the world of today where we are too much depended on computer and more specifically Internet, we are not paying head to the approaching disaster i.e. cyber-crime. Although the first cyber attack took place in 1834 in France but, still we are not paying head to it the most recent one among them was wanna cry. Cyber crime has introduced a total new form of criminals, what make these criminals more dangerous is the very fact that they need not to be physically strong or carry any weapons like traditional criminals. They can have your personal data on their finger finger tips. The good news is that now the government has started recognizing the need of cyber commandos, these cyber commandos are sometimes also referred as ethical hackers. Their main work is to hack the government server with permission from government so as to find the loop hole; if any and sometimes they are also used for offensive attack but still the step taken in this direction is not sufficient and there is lot to be done.
Keywords: *cyber crime, cyber commandos, ethical hackers, cyber terrorism, cyber attack*

Introduction
The world today relies heavily on the need of internet. The introduction of smartphone, desktop, laptop and other devices has increased its value in our day to day life. In present day we can't imagine our world without internet; but this internet has given birth to a total new world called cyber world. This world is both a boon and ban for our society. On one side where it makes our life easy through cashless transaction, simulation, e-governance and many other things; at the same time, it has given birth to the whole new breed of criminal often referred as hacker's or cyber-criminal. Wanna cry, not petya are some of the cyber-attack which resulted in huge loss of money. As a matter of concern cyber-crime is now not limited to economic or money loss now it has moved one step further now it is resulting in death of young children blue whale game is one of those things. Many times, it is misinterpreted that cyber world is for young generation and they have to deal with it the older generation is immune to it and they can't fall into it; as a matter of fact, it is not true. Hackers are using this mentality against the old generation. As per the survey conducted by site named engineering and technology 75% of people aging more than 45 accepted that they have been targeted by spam e-mail; 6% excepted that they have fallen in trap of it; about a quarter of people aging more than 75 excepted that they feel vulnerable although they have excepted that it has made their life easy. All this problem for sure hints towards a whole new dimension of war the "cyber war". Imagine a Scenario where government of a country is not left with any other choice than war. In this case if they go for full fledge war and even if they win war they will suffer huge loss of life, money, resources and inflammation. On other hand if the same country goes for cyber war than the not just save their resources and people but also gains money, wealth and depletion of enemy country economy without wasting a single bullet. INDIA is not an exception to this; INDIA can may face a cyber war or cyber threat to tackle with such situation we need cyber commandos who can not only tackle such situation but also counter attack if needed. Clearly, it's time for fourth generation war where battle will be fought in cyber world and the fate of the world will be decided there. Gone are those days when battle where fought on the ground now is the time of cyber world we need cyber commandos and ethical hackers to save ourselves.

Literary survey

Taylor [1] has stressed the importance of discovering the different types of cybercrime taking place in today's world i.e. Digital crime and digital terrorism. With the increase in terrorist act committed using computer technology. He has addressed the problem of hacker's and other other type of digital criminal. He also discussed about the different strategies and legal option to tackle them. He emphasized on the need to address the problem of cyber terrorism and information warfare. D. Halder [2] believes that majority of the cybercrime committed against women is due is due to the absence of proper legislation. Art 17 of international covenant on civil and political rights (1996) which prohibits "arbitrary or unlawful interference with privacy, family, home or correspondence or unlawful attacks on honor or reputation". Section 509 of IPC prohibit words, gesture or act intended to insult the modesty of women but this law is not able to protect effectively the rights of women in cyber space. Nykodym [3] considers that the cyber-crime is increasing at a very high speed and the progress made in this direction to tackle cyber-crime is not sufficient which has created a large gap in legislative compatibility across international the globe. The very idea that an individual committing crime in cyber space may not fit in a certain classified branch of criminals but evidence suggest that certain distinguish characteristics cyber criminals may exist in cyber space. The most common among all is the cyber-criminal inside their own wall. Broadhurst [4] explores the nature of groups engaged in cybercrime, he outlines the definition and scope of cybercrime or cyber offenders. The paper gave example of known cases and motivation of typical offenders, which includes state offenders. The cybercrime committed by state actor, appears to acquire leadership, structure and specialization. By contrast, protest activity tends to be less organized with weak chain of command. Britz [5] has stressed on the creation of unparallel opportunities for commerce, research, education, entertainment and public discourses. The increase on reliance on digital technology and communication. Many undergraduate students rely on internet for source of knowledge but, unfortunately the quality and and authenticity of material available on internet often comes under question. A person sitting in Madagascar can easily stalk a girl sitting thousands of kilometers away or he can share the blue print of weapon of mass destruction while enjoying all the comfort. Mc Cusker [6] has stressed on law enforcement prospective to control traditionally organized group in cyber space, however it is not clear wether or not any any such group exist or not. One thing which is for sure is that it is organized when it is targeted at a particular person or group of people. The critical question questioniewether the introduction of cyber crime has facilitated traditional crime or it has created a total new dimension. He pointed out that there is very less state of apoplexy within law enforcement agencies . He believed that there is very thin line between organized cyber criminals and criminals who simply operate in online space. Lewis [7] stressed on the role of mass media in extension of information through entertainment. He emphasized more on fraud, organized crime and terrorism; which lead him to think about the unwillingness of establishment to tackle it and the hierocracy of businesspeople or politician. The presence of lobbyist media and NGO increases the liable risk involved in cyber space. Business done today through technology i.e. cashless transaction and others are technologically vulnerable, and these affected business people are neglected by traditional media. David wall [8] stressed on the slow response of criminologist. He pointed out that in today's world it is not difficult for a 16-year-old to become the world's largest threat after Adolf hitler and that too without leaving his comfort chair. How we respond to them remain unanswered. He stressed on the on the importance to give rise to the cyber-crime justice system. Bhatt [9] stressed on the origin of cybercrime to the growing

dependence on computers in modern life. While it has bought remarkable change in our life subsequently it become popular as cyber world. It is surrounded by number of things in which crime is the most serious threat. Harcourt [10] has stressed on the major analysis of emerging cultural characteristics of women's activities on the internet across the globe, it brings together communication expert, development worker's and media analyst and women movement. It maps both social, economic and political biases in which the culture of cyber space is imbedded as well it's revolutionary potential explores women's knowledge. It rethinks the very idea of culture by looking at the link and discontinues between the local and global cyber culture.

Findings

Today different type of cyber crime has started taking place like cyber stalking, cyber terrorism, data theft and many others. Women's are the easiest targets in this type of case this is due to lack of legislation. As per article published in India Times dated July 25, 2017 banks lost 88553 per hour due to cyber crime in last 3 year. Traditionally armed forces of any country consist of three components i.e. Army, Navy and Airforce but now in the changed world a fourth component is added i.e. cyber commandos, both for offensive as well as defensive purpose.

Recommendation and Conclusion

Before writing this research paper I was sure that cyber crime is a big challenge for today's world and the only solution for this crisis is cyber commandos. Now after writing this research paper I can conclude that my assumption was correct. In this field there is huge scope of research and development so as to tackle the cyber criminals.

References

Bhatt, S. C., & Pant, D. (2011). Cyber Crime in India. *International Journal of Advanced Research in Computer Science*, *2*(5).

Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction, 2/E*. Pearson Education India.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime.

Halder, D., Jaishankar, K., & Jaishankar, K. (2012). *Cyber-crime and the victimization of women: laws, rights and regulations*. Hershey, PA: Information Science Reference.

Harcourt, W. (Ed.). (1999). *Women@ Internet: Creating new cultures in cyberspace*. Palgrave Macmillan.

Levi, M. (2006). The media construction of financial white-collar crimes. *British Journal of Criminology*, *46*(6), 1037-1057.

McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change*, *46*(4-5), 257-273.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review*, *21*(5), 408-414.

Taylor, R. W., Fritsch, E. J., &Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Wall, D. (Ed.). (2003). *Crime and the Internet*. Routledge.