OPEN ACCESS
Freely Available Online

JOURNAL OF ADVANCED FORENSIC SCIENCES
ISSN NO: 2692-5915

Review

DOI: 10.14302/issn.2692-5915.jafs-20-3204

Term Paper on The Nature of Cyber Crime and Cyber Threats: A Criminological Review

Md. Ashraful Mozid[1,*], Nelufer Yesmen[2]

[1]Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail -1902, Bangladesh

[2]Assistant Professor, Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail -1902, Bangladesh

Abstract

Cybercrime is one of the fastest-growing criminal activities in contemporary age. The first recorded cybercrime happened in France in the year 1820. It was not as sophisticated as cybercrime we know in our world today, but, still, that was a crime. Cybercrime has evolved globally as the online platform is progressing. While progress is made in the battle against cybercrime there still remains a wide gap in the consistency of laws across international borders. The main objectives of this study are to explore the nature of cybercrime in developing countries, find out the cyber threats for terrorist activities and explain cybercrime and threats from criminological aspects. This is a descriptive study which is based on secondary data. This study is based on previous researches & studies. this paper discusses the nature of cybercrime in developing countries. It could allow developed countries to understand better the national and international effects of that cyber threats, to determine the conditions of current regional and international agreements, and to help countries create a sound legal framework. And then we notice the impact of cyber threats all over the world. At last, we discuss cybercrime from criminological point of view. Cybercrime is not limited to two neighboring countries and cross-border conflicts; an attempt could be conducted from another world. It is fearful to see cyber wars as the easiest way to carry out sabotaging rather than wars such as cold war, chemical and biological wars, terrorist wars or jihadist attacks. The international legal framework aims by the International Criminal Court to keep offenders accountable for their actions. The government has by far the biggest burden and obstacle in raising knowledge of cybercrime among the people.

Corresponding Author: Md. Ashraful Mozid, Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail -1902, Bangladesh. Email: ashrafulmozid@gmail.com

Keywords: Cybercrime

Received: Sep 14, 2019 **Accepted:** Jan 14, 2020 **Published:** Feb 07, 2020

Editor: Suleyman Korkut, Department of Forest Industrial Engineering, Forestry Faculty, Düzce University, 81620 Düzce, Turkey.

Introduction and Background of the Study

Cybercrime is one of the fastest-growing criminal activities in contemporary age. The first recorded cybercrime happened in France in the year 1820. It was not as sophisticated as cybercrime we know in our world today, but, still that was a crime. The fact is that the sophistication of crime in cyber space has grown very rapidly from time to time. If ten years ago people committed cybercrime in a much simpler activity known as computer crime, now people committed cybercrime in a much complicated crime such as phishing, carding, probing, stalking, virus attacking and many other illegal activities with unfamiliar names [1][2][3]. Cybercrime may include conventional criminal activities such as stealing, fraud, falsification, slander, and mischief, all of which are subject to a country's criminal laws. Computer misuse has also given birth to a range of new age offenses that the special laws introduced to penalize such crimes are combating. For example, Bangladesh describes those offenses which are not protected by the penal code in Tatha O Jogajog Projukty Ain,2006 [4]. And so it is possible to say that the 1860 Penal Code is insufficient to counter cybercrime. One of the emerging problems of today's world is combating cyber crime with a global population of up to 7,5 billion and an Internet population of 42 percent. Users also may be puzzled about how cybercrime is classified. While this definition is rather vague, cybercrime refers to illegal actions performed using an online means or directed at a computer-based platform because of the relative area of creativity or lack of a measurable existence. Similar definitions are used for cybercrime identification. It can be broadly defined by the introduction of computer technology as a criminal offense created or made possible. Although it seems to be a simple task, it is not easy to define cybercrimes. The difficulty lies in determining clearly what cybercrimes should be treated as. No globally accepted cybercrime concept exists [5].

Girasa (2002:68) provides a slight different definition on cybercrime. Girasa defines cybercrime as a criminal activity in which computer is used as the main component. This definition is indeed similar with the previous definition. The only difference here is the use of computer as the main component, not as the main tool as what Forester and Morison suggested. The word component is not far in its meaning with the word tool. Both mean part of something which is used to help people doing thing. Therefore, the first and second definition is considered not clear enough to define cybercrime [6]. Tavani defines cybercrime as a criminal activity which is only possible to be done with cyber technology in a cyber space. This definition gives clearer boundaries of cybercrime. Activities such as making computer viruses and spreading them through internet is definitely a cybercrime, meanwhile pornography through internet is not purely a cybercrime. Based on the definition, it is still possible for people to spread pornography by using other media such as CD or DVD [7]

Cybercrime has evolved globally as the online platform is progressing. While progress is made in the battle against cyber crime (especially with the Cyber Crime Agreement of the Council of Europe), there still remains a wide gap in the consistency of laws across international borders. The bombing in Times Square in 2010 would be a good example of the extremist use of the internet as a powerful tool. Central to this plot was Faisal Shahzad. Shahzad used public web cameras to conduct reconnaissance of his targets [8]. In 2005, Younis Tsouli, a London-based Moroccan immigrante imprisoned for distributing bombs and propaganda from al Qaeda, used cybercrime to fund his work. A web of websites and forums of Jihadist propaganda were developed by Tsouli and his associates on servers which Tsouli compromise [9].

For one individual case, ISIL supporters in the United Kingdom have been using social engineering to get pensioners off £ 160,000. The proceeds from this project is believed to be used to finance their journeys to Syria and Iraq to enter and fight ISIL [10]. U.S. companies spend about $67 billion every year struggling with electronic fraud and malware systems like viruses and spyware, according to federal Bureau of Investigation's figures. The Irs, the Justification and National Crime Center also reports a gross $559 million per year for a variety of frauds, including defrauds seeking advance viability in conjunction with substantial returns from the bogus lottery or assets, non-fulfillment of goods or payments, and other opponents. The FC3 also calculates a loss amount of $559 million per month for fraud. The figure has dramatically doubled by an additional $265 million in 2008 each year, as in 2009 [11].

As a poor country like Bangladesh face this problem seriously. Recently this problem is increasing rapidly. Although various steps are taken by the government to stop this crime, they cannot become successful. The subject matter of the study is to explain how criminals helps\ increases cyber crime. Now cyber crime has become a crucial problem in Bangladesh. It is increasing day by day. Though this is a serious problem in Bangladesh, there are a few people on this topic. So, it is essential to work on Cybercrime. It will help us to know about the causes of cybercrime in Bangladesh [12]. The Police Headquarters have confirmed that from 2012 to June 2017, there were 1417 cases brought under the Cyber Security Act 2006. In 748 these incidents, the police brought complaints and issued final reports for 179. Of these 19 cases, 48 in 2013, 149 in 2014, 303 in 2015, 546 in 2016 and 352 in 2017 were filed by June 2012, 19 were filed in 2012. According to the Police Criminal Investigation Centre (CID), various police departments are focused on cybercrime. Moreover, CID alone has a forensic laboratory to help detect or prosecute these crimes. When it opened in 2013, the unit registered 25 complaints. Then it rose to more than 70 in 2014. In 2015, there were 217 complaints, in 2016 there were 575 and until July there were more than 600. The bulk of the alleged victims were women. The counter-terrorism and transnational crime (CTTC) cybercrime unit stated that they have received over 500 complaints since the unit was launched, including cases filed after 150 inquiries. Another 55 cases were under investigation [13]. There are several theories in the area of criminology which attempt to explain why some people have deviated, while others refrain from it. While these ideas were originally intended to describe crimes in the "real world," they can still be used in the field of cybercrime. These include theory of social learning, poor self-control theory, general pressure theory, concept of anger, daily task theory, and theory of avoidance of crime. In this article, elements of these hypotheses are explored in order to determine the best explains cybercrime. According to a study performed by Shirley McGuire (McGuire,1997:47) a specialist in psychology of the University of San Francisco, the majority of teenagers who hack and invade computer systems are doing it for fun rather than with the aim of causing harm. Shirley McGuire said that the motives of teens are often unclear to adults. In the region of San Diego, she carried out an open project and asked about 4,800 graduates [14]. At the American Psychological Association Convention her findings were discussed.

- 38% of teenagers were involved in software piracy;
- 18% of all children who have admitted that they are accessing and using the data stored on other personal computers or websites
- 13% of all respondents said that device or data file changes have been made.

The study revealed that just 1 in 10 hackers wished to do some damage or earn money. Many youth carry out illicit machine excitement acts to get excited. Now, many cyber policemen worry more about Orkut as many fake profiles are generated and therefore contribute to crime [14].

To investigate the actions of cyber criminals, Kshetri (2005) uses psychology, culture, international relations and warfare. He notes that the various kind of network attacks vary from countries worldwide in terms of regulative, legal and cognitive validity. Symbolic significance and criticality, the digital value degree and defense defense weakness are part of the cyber criminal's selection criteria for the target networkThe most serious risks to information protection have been identified by Riem (Anthony Riem, 2001:37) not outside criminals wanting entry but by employees, consultants and contractors working within the organization [15].

Freda Adler(1991:79) said that, technology criminals creates their own forms of crime by using computer as an instrument of crime tool to commit attacks on the information: such as thefts of information thefts of services and even traditional crimes such as child pornography, confidence schemes and illegal gambling [15]

N.V.paranjape (2008-09:141) expressed that, Intellectual property crimes and also indicated on blackmailing based on information gained from computerized files such as personal history, sexual preferences, financial data, medical information and so on.

This research helps to find out how cyber crime become a new threat to security and cyber criminals enhances cyber crime. And it may be expected that the research findings will describe the perfect scenario of cyber crime which is caused due to many problems. The research has a great socioeconomic and policy value as well as in the practical application [16].

Objective of the Study

The main objectives of this study are-

- To explore the nature of cybercrime in developing countries.
- To find out the cyber threats for terrorist activities
- To explain cyber crime and threats from criminological aspect

Methodology

Methodology is a set of step to perform a particular task. Methodology involves with the sources of data, analytical review, findings and recommendation. This is a descriptive study which is based on secondary data. This study is based on previous researches & studies. Data has been collected from journals, articles, books, reports, newspapers, publications and some authentic websites. All information are collected according to research objectives.

Findings

Findings of the study describes according to their objectives. At first, this paper discuss about the nature of cyber crime in developing countries. It could allow developed countries to understand better the national and international effects of that cyber threats, to determine the conditions of current regional and international agreements, and to help countries create a sound legal framework. And then we notice the impact of cyber threats all over the world. At last we discuss about the cyber crime in criminological point of view.

The Nature of Cybercrime in Developing Countries

The quick digitalization has taken place in developing countries such as Botswana, Bangladesh, Kenya, Mozambique, Myanmar, Rwanda, and Tanzania. In Asia the rapid growth in internet use, including 10 times or more access increases in China, Indonesia and India since 2002, has also been associated with significant cybercrime increases. The majority of the UN Sustainable Development Goals now include digitalization. International organizations and donor countries continually utilize digital technology as their development goals–social, political and economic. In the background of the Budapest Convention of 2001, the law-enforcement reaction is quickly analyzed throughout Asia. They describe the nature of cybercrime, and equate the laws and regulations in Asian countries with the terms of the Convention. It covers the' beard' or the material and the illegal products such as botnets. While issues arise around cloud computing, social media, wireless / smart phone apps, and other developments in digital technologies, the difficulties of creating successful cross-border cyber criminal's surveillance in Asia also are dealt with [17]

As most cybercrimes are transnational, disparity in legislation and regulations across the country's frontiers renders collaboration in cross-border cybercrimes particularly difficult for governments. As Katyal (2003:180) pointed out, it is increasingly difficult for many countries to extend their national legislation to practices that are considered offensive or detrimental to local taste or community. The world's Internet users in March 2011 were projected to be 2,95 billion (Miniwatts Marketing Group, 2011). Throughout Asia and the Pacific area (i.e. Asia and Oceania) among all Internet users, 45 percent are based. In the Asian and Pacific world, China is home to nearly half of internet users [18]. India is the second largest, currently 100 million Internet user, led by China, Korea (South Korea) and the Philippines. Countries like Japan, South Korea, Taiwan, Singapore, Australia and New Zealand have over 70% of their total internet users online, while fewer than 10% of the people are involved in developing countries such as India, Pakistan, Sri Lanka, Bangladesh and Nepal. The finding of strategies to respond and solutions to cybercrime threats, especially for developing countries, is a major challenge. A comprehensive anti-cybercrime strategy generally contains technical protection measures, as well as legal instruments [19]. Developing countries will implement protection measures into the Internet roll out from the outset, as while the expense of the Internet services may initially increase, the long-term benefits in mitigating cybercrime costs and disruption are substantial and far exceed any potential spending on technological protection measures and network protections [20]. Nevertheless, because of their lower standards of security and safety, the risks associated with the weaker legislation may impact developing countries more significantly (ITU Anti-Spam Legislation Survey 2005, "p. 5). Customers and businesses must not only be covered by conventional firms, but also by online companies or Internet companies. Failure to secure the internet may contribute to significant problems in developing countries fostering the development and inclusion of e-business in online services. For both advanced countries and developing countries, the implementation of strategic initiatives to support cyber security and effective anti-crime regulation is important. Developing countries have to put their counter-cybercrime policies in line from the start with international standards (Spam Issue in Developing Countries 2005, page 4).

Developing countries such as Bangladesh lack sufficient natural resources and try to achieve economic development by using the ICT sector. Throughout recent years, a growing number of countries have explored ICT resources, established guiding principles and developed a national ICT plan as part of the overall National Development Strategy. In particular, ICT has been a key player. ICTs are the main drivers of socio-economic development for Bangladesh (Clause 1.3 of the National Information and Communication Technology (ICT) Policy October, 2002). Experts from IT say nearly 90% of cybercrimes remain unreported. The condition is deteriorating every day for Bangladesh. Bangladesh reports the most recent cyberattacks and crimes:

1. Blackmailing girl by capturing their nude photographs and video on the sly and threatening to expose publicly. Such incidents are caused frequently by their boyfriends and others.

2. There have been various Community platforms used by girls and boys to share telephone numbers for sharing secret video or even nude images, and so on.

3. Hacking in the website of Bangladesh Computer Society, which took place after a few days of a 3 day-long 'Regional Seminar on Cyber Crime' in Dhaka (www.cnewsvoice.com).

4. E-mail threatening the current Prime Minister Sheikh Hasina from a cybercafe (www.thedailystar.net).

5. Hacking into the Internet account of Barisal DC office in 2003 AD, the incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Tar and Telephone Board (BTTB) [The Daily Star, Sunday, July 13, 2003]

6. Hacking took place in the website of Bangladesh Rapid Action Battalion (RAB) in 2008, during the access to www.rab.gov.bd, the website read: "Hacked by Shahee_Mirza." (www.thedailystar.net).

7. Hacking the mail of BRAC Bangladesh.

8. Stealing the transaction report of Dhaka Stock Exchange through hacking.

Once the internet was established, the founding fathers of the internet had little idea that the internet was also misused for crime. Nonetheless, it's happening all over the world, loosely and mostly. The problem now is whether such offenses can be dealt with using traditional or exceptional approaches.

Cyber Threats For Terrorist Activities

In the 90ies, a discussion focused on network based attacks on critical infrastructure ("cyber terrorism"), such as the use of information technology and transport and energy supply in armed conflicts, took the form of "cyberwar" network use by terrorist organisations. The use of computer technology as well as cyber-dependent violence has become more common challenges from terrorist groups. The notion that terrorists might result in a massive death loss, global economic mess or destruction of the world through piracy of critical infrastructure networks caught public imagination. national imagination. Cyber terror acts are known to be a potential target for air traffic control facilities, nuclear power plants, electricity grids, schools and equity markets. The notion is not simply to create a new generation of cyber terrorism, but to strengthen the capacity to conduct a destructive cyber-attack, for example by Islamic State, Al-Qaeda or a certain known terror organization. "In today's world", according to former US President Barack Obama, "acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer—a weapon of mass disruption." What we do know, on the other hand, is that terrorist organization's use the internet on a daily basis for a range of activities including propaganda, recruitment and communication. Islamic State has shown particular prowess in using social media to inspire vulnerable individuals around the world to join its cause. These uses of technology by terrorist groups pose major challenges and should remain the focus of cyber security efforts in counter-terrorism [21]. Network protection vulnerabilities have been demonstrated clearly by the proliferation of viruses and botnet assaults. Successful militant internet attempts are probable, but the significance of risks is hard to assess (Terrorist Capabilities for Cyberattack, 2007, page 13). Typically, the style of terrorist activity which characterized the beginning of the 21st century was planned to prepare high-mortality incidents, to attain radical groups ' targets and both the power of the attackers and the weakness of the fired population. Such attacks often attract lawmakers ' attention to and goad acts that could be used to boost the group's credibility and recruit new members for radical causes. The social and political success of such efforts in post-9/11 environment has only increased the trend (The Future of Terror, Crime, and Militancy, page 239 *etseq).* Everything shifted after the bombings on September 11, which contributed to the beginning of an extensive discourse on the use of ICTs for attackers. Saying that the perpetrators were using the Internet to plan the assault encouraged everything debate (http://www.aci.net/kalliste/electric.htm.). While the assaults were not cyber-attacks, the Web played a role in the planning of the 9/11 assault as the party who did not perpetrate a web-based attack. Different ways terrorist organizations use the Internet have been found in this context (CNN, News, 04.08.2004) [22] Today, it is known that terrorists use ICTs and the Internet for:

- Propaganda
- Information gathering
- Preparation of real-world attacks
- Publication of training material
- Communication
- Terrorist financing
- Attacks against critical infrastructures

Many terrorist organizations depend on third-party financial resources. Following the 9/11 attacks, tracking this financial transaction has become one of the main ways of combating terrorism. The reality that financial means required to conduct attacks are not inherently high is one of the main problems in this regard (CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4). Web services can be used in many forms to fund terrorism. Terrorist organizations may use electronic payment systems to make donations online (Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253). You can use websites to publish information about donations such as which bank accounts for transactions should be used. The Hezbollah Tahrir organization, which publishes bank account data for potential donors, was an example of this approach. (*Weimann*in USIP Report, How Terrorists use the Internet, 2004, page 7). The Irish Republican Army (IRA) was one of the first terrorist organizations, which collected donations through credit cards. Another approach is to donate credit card online (Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4) [23]. All methods involve finding and monitoring financial transactions using the information published. Anonymous electronic payment systems are therefore likely to become increasingly popular. The fact that cyber warfare is an evolving danger must be mitigated. The population of digital devices is growing rapidly, rendering them the first-line susceptible to a cyber-attack. A prerequisite assumption therefore is that our own enemies have to reassess cyber-attack on a regular basis over time because of the emergent existence of the digital economy, technology technologies, and skills (The Future of Terror, Crime, and Militancy, 2001, page 42).

Cybercrime and Threats From Criminological Aspects

Cyber-reality is extremely paradoxical from a criminological perspective. Deviancy and violation of "normal" practices and values is part of all phases of cyber-space development. Professional innovation has achieved primary importance among hackers only because the idea of exclusivity, anonymity and copyright transcended their community. Cyberspace transparency has always been culturally determined and an intrinsic feature of the hacker culture. Cyber crime is committed electronically, and is often not clearly linked to any geographical position, unlike conventional crime committed in one geographical location. A concerted global solution to the cybercrime issue is therefore required. This is mainly because there are a number of problems that hinder effective cybercrime reduction. The weaknesses in technology, law and cyber criminology present some of the major issues (Professor Hamid Jahankhani*,2003:13).*

Most criminal viewpoints describe criminality on the physical, economic and environmental aspects, and see crime as happening in a single geographical location [24]. The description of crime allowed crime to be identified and ultimately adapted for the specific target group for crime prevention, monitoring and calculating approaches. This function, however, cannot be conducted. As a consequence, it is virtually impossible to identify areas of identifiable offenses that cause cybercrimes. In addition, this makes the criminal viewpoint worthless on the grounds of spatial variations (Brvar, 1982:92). Criminology thus encourages the motives of offenders to be identified by examining the social traits and position of perpetrators, which helps explain whether crimes committed by individuals with particular characteristics are widespread (Computer Crime: A Criminological Overview,2001:35). But in the case of cybercrimes the association of widespread acceptance of conventional crime with social exclusion and criminality can not be valid and cyber criminals, like traditional criminal perceptions, are quite' atypical.' There are therefore no useful explanations for cybercrimes from the current perspectives of criminology which connect marginalization and social exclusion to crime. Unless the causes are known, effective measures to combat cybercrime can difficultly be implemented by law enforcement agencies and the government (Levi, S. 1984). Hackers: Heroes of the Computer Revolution).

Self-Control and Space Transition Theory

K. Jaishankar has developed a theory called 'Space Transition Theory'in order to explain the causation of crimes in the cyberspace. I felt the need for a separate theory of cyber crimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon of cybercrimes (Jaishankar 2008). He published this theory as a chapter in a book titled "Crimes of the Internet" edited by Frank Schmalleger& Michael Pittaro, published by Prentice Hall (2008: 283-301). "Space Transition Theory" is an interpretation of the essence of people's behavior in physically and on a cyberspace which demonstrates their conformity and non-conformity (Jaishankar 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Theory of space transfer suggests that when they shift from place to room, people act differently. The concept is nowadays, as is probably the most widely discussed in cyber crimeology, a significant scientific principle in criminal literature. This hypothesis discusses the creation of cyberspace as a new venue for criminality and describes the origin of cyberspace crimes (Jaishankar, 2008). The advancement of the concept of space transfer played a key role in the creation of cybercrime hypotheses. Because it came at a time when no other social scientist was able to explain as clearly as Jaishankar the overarching trend of cybercrime.

Propositions of Space Transition Theory

1. 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.

2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime.

3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.

4. Intermittent ventures of offenders in to the cyber-space and the dynamic spatiotemporal nature of cyberspace provide the chance to escape.

5. (a) Strangers are likely to unite together in cyber-space to commit crime in the physical space. (b) Associates of physical space are likely to unite to commit crime in cyberspace.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

Because criminology has begun to see the rise of cyberspace as a major focal point for criminal activity, a new theory is needed to explain why cybercrime is happening. The above principle of spatial transformation outlines the criminal conduct in cyberspace. The Space Transformation Theory needs to be tested to figure out if it addresses cybercrime [25]. The second issue of the paper includes a wide range of articles written by emerging and established experts in the field of cyber criminology. The first essay by Russell Smith explores how developments in ICTs have created new crime problems, but also helped to prevent, track, evaluate, prosecute and execute abuse. Michael L. Pittaro's second article is a guide to online harassment and intimidation, which is called cyberstalk. In this article he addressed how the internet has encouraged violence. He claims that cyberstalking is not so simplistic but an evolution of online harassment as conventional stalking. The author gives several examples of cyber stalking and how the suspect is quickly abused. Each problem includes two book reviews. Nicholas Chantler, of Queensland University of Technology reviewed the book titled "CYBERCRIME–The Reality of the Threat by Nigel Phair. He believes that this book is an easy-to-read document for addressing cybercrime, based on the experience of the writer as a federal agency at the Australian Crime Centre and an Australian Federal Police. He notes that Internet users who get filmed on the site of on-line crime will decrease their trust in e-commerce[14]. The profile of cybercrime criminals is also mentioned briefly. Often identified are the global analyses of the elements of cyber crime. The book discusses cybercrime under a broad range of headings-recommendations for and expectations for the law enforcement action-such as unauthorized malware, crime of identification, phishing, critical infrastructure security, intellectual property, messaging, terrorism and compliance.

In fact, versatility, dissociative privacy, easy online communication and lack of protection are attracting more and more conventional offenders to the Web. In this analysis also the theory that cyberspace is used by cyber criminals if there is a discrepancy between the principles and values of physical space [26]. Although few scholars test the theory of space transformation, there are some issues with the feasibility of testing the theory and several scholars have underlined this (Holt, Bossler, &Spellar, 2015; Holt &Bossler, 2016). It is to be noted that getting data of the cyber crime offenders is an onerous task and hence the difficulty of testing the space transition theory ensued. Even, Kethineni, Cao and Dodge (2017, pp-13-14) note that: While case studies provide some evidence for space transition theory, further data is needed to empirically evaluate these ideas. "Having a large population of cyber criminals will be challenging at this point and this problem may be addressed in the future [27]. Cybercrimes will continue to grow, and in the future there is a thin line between offline and Web criminals, which will allow more cyber offenders and will make testing the hypothesis of the space transformation far simpler than is currently the case.

Conclusion

Cyber crime is not limited to two neighboring countries and cross-border conflicts; an attempt could be conducted from another world. It is fearful to see cyber wars as the easiest way to carry out sabotaging rather than wars such as cold war, chemical and biological wars, terrorist wars or jihadist attacks. Crime involving a machine or a cybercrime includes any crime involving a device and a network. The machine may or may be the subject of the crime committee. Dr. DebaratiHalder and Dr. K. Jaishankar (2011) defines Cybercrimes as: "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 (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" [28]. These offenses that endanger the protection and financial health of a country. Issues related to these types of crimes have become popular, particularly ones related to breaking, copyright violations, child pornography and childcare. Privacy problems also occur when confidential information is legally or otherwise lost or intercepted. Internationally, cybercrimes are perpetrated by both states and non-state actors, including hacking, financial fraud, and other cross-border offences. Operation that crosses international borders and affects the desires of at least one nation state is sometimes referred to as cyber warfare [29]. The international legal framework aims by the International Criminal Court to keep offenders accountable for their actions. The government has by far the biggest burden and obstacle in raising knowledge of cybercrime among the people.

References

1. http://thedailynewnation.com
2. http://www.thedailystar.net
3. http://www.bangladeshobserver.com
4. Information and Communications Technology Act, 2006
5. Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society. New York: Oxford University Press, 2009
6. Grabosky.Peter. and Smith. Russell,Crime in the Digital Age:, Sydney: Federation Press, 1998 (co-published with the Australian Institute of Criminology).
7. Levi, M. (2001). Between the risk and the reality falls the shadow: evidence and urban legends in computer fraud. In: D. S. Wall (ed.), Crime and the Internet. London: Routledge.
8. www.ticklethewire.com
9. www.washingtonpost.com
10. http://www.dailymail.com
11. The IC3 2009 Annual Report on Internet Crime. Washington, DC: Federal Bureau of Investigation, 2010
12. http://daily-sun.com
13. https://www.dhakatribune.com
14. Smith, R. G., Holmes, M. N. &Kaufmann, P. (1999). Nigerian Advance Fee Fraud., Trends and Issues in Crime and Criminal Justice, No. 121, Australian Institute of Criminology, Canberra (republished in The Reformer
15. Longe, O.B., (2004). Proprietary Software Protection and Copyright issues in contemporary Information Technology. (M.Sc Thesis) Unpublished. Federal University of Technology, Akure, Nigeria.
16. Paranjape.N.V.(2008). Criminology and Penology, 13th ed., Allahabad: Central Law Publications.
17. http://www.ejisdc.org
18. Grabosky, P. (2001). Computer Crime: A Criminological Overview. V: Forum on Crime and Society, vol. 1, no. 1. New York: United Nations Publications, p. 35–53.
19. http://www.osce.org
20. World Information Society Report 2007, page 95
21. http://www.internationalaffairs.org
22. https://edition.cnn.com
23. Turkle, S. (1997). Life on the Screen: Identity in the Age of the Internet. New York: Simon & Schuster.Wall, D. S. (2007). Cybercrime: The Trasformation of Crime in the Information Age. Cambridge, Malden: Polity
24. Aghatise E. J. (2006): Level of Awareness of Internet Intermediaries Liability. (HND Project work) Unpublished. Auchi Polytechnic, Auchi, Edo State, Nigeria.
25. Jaishankar, K. (2008). Space Transition Theory of cybercrimes. In Schmallager, F., &Pittaro, M. (Eds.), Crimes of the Internet.(pp.283-301) Upper Saddle River, NJ: Prentice Hall.
26. R. K. Chaubey.(2009). An Introduction to Cyber Crime and Cyber Laws, 1st ed., Kolkata: Kamal Law House.
27. Naughton, J. (1999). A Brief History5 of the Future: The Origins of the Internet.London: Phoenix.
28. Ahmed. Zulfiquar. (2009). A Text Book on Cyber Law in Bangladesh, 1st ed., Dhaka: National Law Book Company.
29. Halim, Abdul.& N. E. Siddiki.(2008). The Legal System of Bangladesh after Separation,(1st ed.), Dhaka: University Publications.