A Social Review on Nature & Reason of Cyber-Crime and the Laws Regarding Prevention in Bangladesh

Khondokar Hafijur Rahaman[1], Md. Abul Hasam[2*]
[1]*Journalist, the Daily Janakantha, Dhaka, Bangladesh*
[2]*Department of Sociology, Primeasia University, Dhaka, Bangladesh*
*Corresponding author**

Abstract: **This paper tries to identify the nature, reason and prevention laws of cybercrime in Bangladesh. The study followed the qualitative technique and data collected from secondary sources. Cybercrime is a worldwide social phenomena in present technological era as the scientists, engineers and law enforcing agencies are getting very serious regarding security and safety of mass use of technological apparatus specially computer and internet. It covers such a broad scope of criminal activity; the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in many ways, it is unfortunate that people also use these technologies to take advantage of others in unfair ways. Even after taking many protective and preventive measures, the crime is out of controlled. Therefore, it is smart to protect yourself by using antivirus and spyware blocking software and being careful where you enter your personal information. Overall cyber means committing any crime by using computer, information technology or any act which is forbidden by law. The study may help the policy makers and government personnel who take initiative to protect and prevention the crime of a society.**

Keywords: **Cybercrime, Nature, Reason, Prevention, Cyber law, Social Awareness, Bangladesh.**

I. INTRODUCTION

Information and Communication Technologies (ICT) have transformed modern lifestyles in different ways. These have provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. Cyberspace has supplemented, if not substituted, functions and services ranging widely from routine personal life to national and global affairs. The massive convenience offered at an astounding speed dissolving all spatial limits make cyberspace indispensable to a modern world that is still at pains to fathom its potential. As dependence increases on technology, so does vulnerability due to its abuse. It has also led to vast quantities of malware and spyware circulating freely on the Internet, and an alarming rise in the number and scale of cyber criminals [1].

Cybercrimes, generally involving computers and networks, are embarrassing governments and individuals; impairing systems; and causing loss of billions of dollars every year. These crimes in reality include copyright infringement, software piracy, and password cracking or cheating by others' ID, cyber pornography, e-mail threats and e-stalking, hacking others' websites and so on. The world is threatened, perhaps, by the worst form of aggression through these crimes. The increased reliance on the Internet by business, government and society makes it a prime target for criminals' intent on disrupting economy and way of life [2].

Cybercrime has grown to be larger than illicit drug sales worldwide and it is estimated that losses from intellectual property to data theft in 2008 ranges as high as $1 trillion. How much is Bangladesh vulnerable to cybercrime; is she aware; and is she ready to respond to this threat and what should she do to counter this? While some studies are carried out about the use and development of the cyberspace, no serious evaluation is done of the nature of threat that is tagged with it, the degree of destruction it can do, or the amount of loss it can incur. At present, the cybercrimes in Bangladesh scenario includes life threatening email to important personalities, malicious mail to foreign diplomatic missions, pornography, fraudulent mail for the realization of money, inserting porno movies to the well-known web sites are a few to name. Much, however, remains unreported, most of which may not have taken a devastating toll yet. When we are envisioning 'Digital Bangladesh', Bangladesh is more exposed to the evils of technological crimes. Unfortunately, we are not much aware of this crime and consequences [3].

This paper attempts to examine our vulnerability, as well as the preparedness, by analyzing the degree of penetration of cyberspace in the country and the nature of threats accompanying it. A conceptual overview, skimmed chiefly out of published materials, is presented at the beginning. The vulnerabilities and preparedness is then evaluated before recounting a response strategy to fight cybercrime. Finally, the paper suggests an outline strategy to deal with cybercrime in Bangladesh.

The overall objective of the article is to identify the impact of cybercrime in Bangladesh with regard to technological enhancement. The primary objective of the study is to make out the real scenario of cybercrime as well as: to explain and examine the cybercrime committed in different sectors, to revisit the legal measures, strategies taken in Bangladesh, to explore existing schemes and mechanisms taken against cybercrime in Bangladesh, to analyze the problems regarding the scheme of the existing cyber legislations, and to make possible suggestions for the protection of cybercrime.

II. THEORETICAL FRAMEWORK

The internet, in general, is perhaps today's most influential technological invention and continues to change daily life for virtually everyone on Earth. A major part of the world people is plugged into cyberspace, and thousands more enter the online world every day. Not only has the Internet revolutionized the way we interact with others and learn, it has forever changed the way we live. As internet and computer technologies continue to thrive; criminals have found ways to use these technologies as a tool for their deviant acts. Cybercrimes are now a new breed of crime that are perpetrated using computers, or are otherwise related to them. Cyber-crime is different and more heinous than conventional crime in that the crime is committed through an electronic medium which makes it difficult to track and identify the criminal. The most common types of cybercrime include cyber fraud, defamation, hacking, bullying, and phishing [4]. Within the field of criminology, a number of theories exist that attempt to explain why some people engage in deviant behavior, while others abstain from it. Although, these theories were originally meant to explain crimes committed in the 'real world', they can still be applied to cybercrime. These theories include social learning theory, low self-control theory, general strain theory, frustration aggression hypothesis, routine activity theory, and situational crime prevention theory. This paper will analyze aspects of the above theories, for the purpose of seeing which best explains the cause of cybercrime [5].

Renowned scholars Akers' social learning theory is a general theory of crime and has been used in explaining a diverse array of criminal behaviours. This work embodies within it four fundamental premises that include differential association, definitions, differential reinforcement and imitation [14]. Social learning theory is based on the idea that individuals develop motivations and skills to commit crime through the association with or exposure to others who are involved in crime (i.e., associating with deviant peers). Akers's proposed that this exposure to deviant behaviour provided individuals with definitions that are seen as either approving of or neutralizing the behaviour. These definitions become rationalizations for criminals when committing a crime. Differential reinforcement refers to the rewards that are associated with a particular criminal behaviour. This criminal behaviour is originally learned through the process of imitation, which occurs when individuals learn actions and behaviour by watching and listening to others. So, when an individual commits a crime, he or she is mimicking the actions that they have seen others engage in [14]. In regards to cybercrime, research has found that social learning theory can explain the development and on-going issue of software piracy. In their study of software piracy, Burruss et al, found that individuals who associate with software piracy peers learn and subsequently accept the deviant conduct. Software piracy requires a certain degree of skills and knowledge to access and deviant peers to originally learn these skills from. Furthermore, the deviant individuals rationalize their criminal behaviour and help in the fostering of a network that connects and teaches other individuals these rationalizations and behaviour. The study also suggested that individuals are more likely to engage in software piracy when they see others experiences positive reinforcement for their participation [14]. Not only does social control theory explain for software piracy, elements of this theory can be attributed in other cybercrimes. For example in any crime, the rationalizations and skills must be learned and behaviour is reinforced through the association and observation of others. Thus, the main idea behind social learning theory is that we become who we are based on our surroundings and this explanation can be used to explain cybercrime.

While social learning theory emphasizes the importance of external factors that influence criminal involvement, low self-control theory posits that low self-control is a key factor underlying criminality. This theory was originally developed by criminologists Michael Gottfredson and Travis Hirschi. They proposed that their self-control theory can explain all types of crimes, all the time [14]. Individuals with low self-control were characterized with being risk taking, short-sighted, impulsive and prefer simple and easy tasks. These characteristics inhibit an individual's ability to accurately calculate the consequences of deviance. According to this theory, crime is seen as a means of obtaining immediate gratification, and the ability to delay such short-term desires is linked to self-control. As such, those with a propensity for criminal involvement are thought to lack sufficient self-control. Also, people with low self-control act impulsively-without much thought and based on what they are feeling at the moment. This makes them risk takers as they do not consider the consequences of their actions. Finally, low self-control people are focused on themselves and lack empathy towards others [14]. According to Gottfredson and Hirschi, low self-control originates in early socialization when parents are ineffective in their parenting. Therefore, neglecting and uncaring parents are likely to fail to socialize their child to properly delay gratification, care about the feelings of others, and restrain their impulses. As a result, children with low levels of self-control end up being more prone to crime, and their criminal propensity continues into later life. The characteristics of low self-control can be applied to some simple forms of cybercrime, including software piracy. In their study, Burruss et al., stated that levels of low self-control are directly related to the act of software piracy. For instance, an individual is likely to perform software piracy because they are impulsive and unable to wait to purchase a copy of the software. These individuals are not likely to be empathetic to the copyright holder and neglect any responsibility. Further, these individuals are likely to be attracted to the thrill and ease of engaging in software piracy. The study also found that low self-control does have an effect on software piracy and that social learning theory measures (i.e., associating with deviant peers and positive attitudes toward software piracy) condition this effect. Thus, from the characteristics of low self-control, those with low levels of self-control are likely to participate in deviant behaviour both on and offline because of their desire of immediate gratification.

Robert Agnew's general strain theory proposes that strain leads to negative emotions, which may lead to a number of outcomes, including delinquency. The specific strains discussed in the theory include the failure to achieve positively valued goals (e.g., money), the removal of positively valued stimuli (e.g., loss of a valued possession), and the presentation of negatively valued stimuli (e.g., physical abuse) [16]. The first strain looks at the gap between the expectations of the individual and what they actually achieve, which leads to disappointment and resentment. The second type of strain is caused when a positively valued stimulus is removed and the result is delinquency. This criminal behaviour may present itself as an attempt to ease or replace the stimuli. The final type of strain occurs when confronted with negative stimuli. This may cause delinquency as a means to terminate or avoid the negative stimuli [16]. According to Agnew, strain does not directly cause crime but rather promotes negative emotions like aggression and frustration. This is directly in conjunction with the frustration-aggression hypothesis by Yale university psychologists. They believed that anger comes before frustration, and frustration can manifest into both aggressive and non-aggressive behaviour [18]. In turn, these negative emotions necessitate coping responses as a way to relieve internal pressure. Coping via illegal behaviour and violence may be especially true for adolescents because of their limited resources and inability to escape frustrating environments. In their article, Patchin & Hinduja, decided that general strain theory can be used to explain illegal behaviour such as cyber bullying among youth.

Cyber bullying is a serious and growing problem that occurs when youth use electronics to harass or intimidate their peers in a deliberate attempt to inflict direct or indirect harm. There are some unique elements in the digital setting that are not present offline, such as: anonymity, constant connectivity, and permanence. This new technology allows victims to be attacked at any time and the anonymity of cyber bullies makes it difficult to identify them. Agnew argues that strain makes people feel angry, frustrated, depressed, and essentially creates pressure for corrective action on the part of the victim. In response to this pressure, victims react by wanting to take a corrective action as a means to alleviate the bad feelings. Consequently for some victims, cyber bullying is one corrective action that adolescents might take to mitigate the bad feelings [16]. Together, general strain theory and frustration aggression hypothesis, provide an understanding of how people, especially youth, respond and deal with negative strain, whether it may be to bully others or do deviant acts to alleviate the strain.

Routine Activity Theory was developed by Cohen and Felson to originally fill the shortcomings in existing models that failed to adequately address crime rate trends since the end of World War II. They recommended that the behaviour of most victims is repetitive and predictable and that the likelihood of victimization is dependent on three elements: motivated offenders, suitable targets, and the absence of capable guardians [17]. The motivated offender is someone willing to commit a crime if an opportunity presents itself. A suitable target is one that the motivated offender values (e.g., credit card information). In addition to these, a capable guardian includes anything that obstructs the offender's ability to acquire the target (e.g., antivirus, encryption). With the increasing use of the internet, criminals have found new opportunities to victimize their targets on a whole new platform. Researchers have found some support for applying the tenets of routine activity theory to the study of cybercrime [19]. People whose regular activities place them in situations where they have the possibility of interacting with offenders are at an increased risk of being victimized. Research has found that the amount of time spent online, more use of internet banking and online purchases, and risky online behaviour make people more suitable to offenders. Individuals with these actions are more likely to be targeted for identity theft. Furthermore, the lack of antivirus and network security (capable guardians) is associated with more victimization [17]. So, routine activity theory can be used, to an extent, to explain certain types of cybercrime.

Situational crime prevention is a crime prevention strategy that addresses specific crimes by manipulating the environment in a way that increases the risk to the offender, while reducing the potential reward for committing the crime [15]. It is rooted in rational choice theory, routine activities theory, and crime pattern theory. Like other prevention measures, situational prevention focuses on reducing crime opportunities rather than the criminals. This theory differs from other criminological theories in that they do not look at why the offender did the crime, but rather how to prevent crime from altering the physical surroundings where the crime takes place. Essentially, it seeks to make the criminal act more difficult to commit in the first place. Like other primary crime prevention measures, situational prevention tends to focus on reducing crime opportunities rather than on the characteristics of criminals or potential criminals. In regards to cybercrime, there are ways in which space can be designed to prevent crime through: target hardening, access control, deflecting offenders, and controlling facilitators [15]. Target hardening is the actual physical (or digital) barriers that reduce chances of crime, such as encrypting sensitive information. Access control involves strategies to prevent potential offenders from areas that a crime can occur. This includes photo ID cards, passwords, and check-in booths. Deflecting offenders is concerned with initiatives to move potential offenders away from their crime targets. For example, storing valuable data off-site would deter potential offenders from searching for it. Controlling facilitators involves checking elements that may cause a crime, such as doing background checks on employees or restricting unauthorized installations on computers [15]. Research has found that situational crime prevention strategies can be used to reduce cyber stalking and other online victimization crimes. Also, prevention strategies can be applied InfoSec to effectively protect the assets of organizations from being exploited online [15]. Theoretically, if used effectively, the principles of situational crime prevention seem to be able to prevent most categories of cyber-crime.

Computers and the internet have become common place in today's society. This new technology has resulted in the development of a new form of crime, cybercrime. I think that criminal behaviour cannot be explained entirely by one theory; it requires the combination of various theories. Different aspects of each theory can be used in conjunction to compensate for what each individual theory failed to explain. For example, social learning theory believes that crime is learned through association with deviant peers and research has already shown that there is a relationship between the number of deviant peers an individual has and his or her participation in software piracy [14]. But, researchers have not examined whether social learning theory applies to all types of cybercrimes or just certain cybercrimes. On the other hand, low self-control theory asserts that low self-control is the cause of crime all the time. This may be true for some criminals, but many criminals, like those involved in white collar crimes, do not adhere to the principles of low self-control. However, while self-control theory is useful in explaining why individuals may act in a certain way, it does not explain the situations that must be met for a crime to occur. Routine activity theory describes the situational factors that must be present for a crime to occur. It is more difficult to apply this theory to cybercrime because the offender and victim do not necessarily have to meet for the crime to occur. Similar to low self-control theory, strain theory maintains that when an individual cannot achieve his or her goals, he or she experiences strain and as a result they may turn to crime [16]. But, researchers could further study whether an individual's strain in the 'real world' affects their deviant behaviour in the virtual world. So, an individual's low self-control and negative strain combined with his or her deviant associations and regular activities can increase an individual's risk of being victimized online. Future studies of cybercrime victimization may draw benefit from using a combination of these theories to explore the problem. Cybercrime research will be important to our understanding of crime as our society becomes more and more dependent on technology.

III. RESEARCH METHODOLOGY

The study followed the qualitative technique and data collected based on secondary sources like Magazines, books, research documents, articles of newspapers and internet sources. The data are interpreted in light of above research objectives using thematic procedure.

IV. DISCUSSIONS

Cybercrime: Cybercrime is the latest and perhaps the most complicated problem in the cyber world. This crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime [6].

A generalized definition of cyber crime may be unlawful acts wherein the computer is either a tool or target or both. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system[7].

Origin of cybercrime: Origin of the cybercrime was from the origin of the computer, which we can say from the era of mainframe computers. Professor Susan W. Brenner in his book Cyber Crime divided the origin of cybercrime in two phases, first from the era of mainframe computers to 1990, when the internet and personal computers were becoming more sophisticated and more pervasive. And the other phase is from 1990 to present. More easily we can divide the origin of cybercrime in two periods, one, before the internet and the other after emergence of Internet, because 1990 was the time when internet was spreading very fast around the globe [8].

The Nature of Modern Cybercrime: Nowadays criminals that indulge in cybercrimes are not driven by ego or expertise. Instead they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work. Cybercrimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber-crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals. Mobile threats**,** particularly from mobile devices are clearly on the rise. As we are all now aware, PC sales are decreasing: according to recent reports, global sales for PC's declined for the fifth consecutive quarter in the

April-June period, which makes that the longest decline in the PC market's history. With the increase of hand-held devices means that there is an increase on attacks directed at the devices [9].

Reasons for the crime: Hart in his work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber-crime. The reasons for the vulnerability of computers may be said to be [10];

Capacity to store data in comparatively small space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier[11].

Easy to access

The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system [12].

Complex

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system [13].

Negligence

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber-criminal to gain access and control over the computer system[3].

Loss of evidence

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation [13].

Problems: Cybercrime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more.

Increased sophistication of cybercrime attacks and vulnerability of information available online is a serious concern for institutions, law enforcement agencies and other stakeholders. Victims of these attacks are not just private citizens or organizations with limited resources available to protect themselves but very large companies [20].

The Act in particular deals with certain offences, which may be known as Cybercrimes. Several studies have attempted to determine the reasons why social network users are unconcerned and unaware of the privacy concerns associated with their online practices, but the reasons prove to be numerous and varied. Gross considers the privacy implications that arise from social networking sites upon their transition from `niche phenomenon to mass adoption. Researchers said the real privacy concerns arise when users allow to unknown people and would not trust to have access to the personally identifiable information they have made available. The authors also explained that the people do this disclosure of information because they are unaware of the large number of people who are allowed to view this information and the implications associated with these viewings. Gross and Acquisti explain that such practices allow 'third parties to create digital dossiers of their behavior'[21].

Similar research has been done by Young and Hasse. They studied the strategies students have developed to protect themselves against privacy threats. The results showed that personal network size was positively associated with information revelation, no association was found between concern about unwanted audiences and information revelation and finally, students internet privacy concerns and information revelation were negatively associated. Based on their findings, they proposed a model of information revelation and draw conclusions for theories of identity expression [22].

In researchers investigated of the privacy settings offered by each website, we found that users are generally unaware and/or unconcerned with protecting their privacy on social networking sites. They have rated Facebook.com 4 because the website limits global far-reaching searches and its platform is user friendly. They concluded the responsibility of providing privacy does not lie to the sites rather privacy should rest solely on the individual users. In Pugh studied computer-mediated environments (personal Websites) to develop theory of how people contemporarily define themselves in their social online space. Author brought the Facebook user celebrity experience through connected networks/fan base, a highly regarded image, and developed associations throughout the analysis. Mazman and Usluel have analyzed the usage purposes of social networks focusing on the possible differences between females and males. These usage purposes can be categorized under four categories, namely maintaining existing relationships, making new relationships, using for academic purposes and following specific agenda. The difference on making new contacts was in favor of males, the differences on the other three user purposes were in favor of females [23].

Cybercrime in Bangladesh

Cybercrime is a contemporary phenomenon to Bangladeshi people. Although presently Bangladesh is not as vulnerable to cybercrime as the developed countries are, but there is little room for complacency. Once 'Digital Bangladesh' comes in reality, we will certainly face the critical situations that are being suffered globally. At the moment, Bangladesh is not aware of her cyber security. Though computer is becoming a common household item and the number of Internet users has already crossed ten million, very few computer-related offences are reported to the police. However, a few of the major cybercrime incidents that bring to the notice of the public , for instance, on 23 August 2004, an e-mail was sent to the Bangla daily Prothom Alo, containing death threat to Sheikh Hasina, the then leader of the opposition in parliament. Two days later, another e-mail received that also contained death threat for Khaleda Zia, the then Prime Minister, her eldest son and some members of parliament. These were the first two incidents of cybercrime. In 2008, the website of the Rapid Action Battalion (RAB) was hacked. The hacker, Shahee Mirza wrote on the RAB website, 'You do not know what the cyber security is or how to protect yourself' (The Daily Star, 6 September, 2008). On 21 March 2010, 19 of the 64 district web portals were hacked, immediately after inauguration by the Prime Minister on 10 January [22].

Social Defamation and Privacy Violation

Exploitation of Social Networking and Chat sites leave our population, especially the younger generation vulnerable to different types of social attacks. Password cracking or cheating is a common crime done by juveniles in Bangladesh. These crimes are mainly committed by doing fun through Facebook [23].

National Values, Belief and Faiths

Bangladesh is all along known to be an embodiment of a moderate society characterized by liberally practicing religious people with high resilience, forbearance, modesty and strong attachment to the traditional culture, values and belief. Malicious and clandestine propaganda through Internet may impair the harmonious social bondage and where people of various faith and sectarian views live in peace and harmony. Teen agers who use Internet have been more prone to pornography than the use of huge scholastic exploration in the domain which is highly antithetical to the mores, faith and values embedded in the society of the country[24].

Matters of Economics and Finance

Although cyber-attacks have caused billions of dollars damage in financial sector, we have yet witness the implications of a catastrophic cyber-attack in Bangladesh. Cyber attackers generally disrupt the banks, the international financial transactions, the stock exchanges. Freddy Tan, Chief security advisor of Microsoft Southeast Asia, said that The impact of cybercrime is not as alarming in Bangladesh because of financial transactions have not yet been fully facilitated online. He warns that as soon as financial transactions are allowed online computer crimes will increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them[25].

Embedded Threats

Modern equipment comprises of number of systems and sub systems, of which embedded systems are used by all critical sectors of economy including Armed Forces. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions [26].

E-espionage and Cyber War

In cyber war computers are simply another tool, to be used by these same people for espionage. Our adversaries may conduct e-espionage on our government, university research centres, industries and Armed Forces. They may also seek to prepare for cyber strikes during a confrontation by mapping our e-governance information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. During crisis, adversaries may seek to intimidate the Nation's political leaders by attacking Critical Information Infrastructure (CII) thereby eroding public confidence in the political system. Bangladesh is utterly exposed to this dangerous espionage threat and we are hardly prepared to combat this[9].

Cyber law in Bangladesh

Bangladesh is planning stringent measures to fight cybercrime amid the rapid expansion of the information and communications technology and telecommunications networks in the South Asian country. Bangladesh's ICT industry has been expanding exponentially and is making its presence strongly felt both in the public and private sectors. More than five million personal computers are now in use in the country with three million internet users, by industry estimates. "We have taken steps to facilitate fair and secured use of information technology as the country lacks a complete law to deal with cyber-crime," says Joint Secretary to the Science and ICT Ministry. Science and ICT Ministry said that the government, which has pledged a "Digital Bangladesh" by the year 2021, had approved in principle to amend previous legislation calling for jail terms and heavy financial penalties to tackle new forms of crime. The proposed law has suggested provisions for a maximum 10 years in jail and taka 10 million (US$150, 000) in fines for hacking into computer networks and putting false and libelous information or indecent material online [6].

The Information and Technology Act, 2006 for Prevention of Cybercrime

The Penal code of Bangladesh contains very few provisions regarding cyber-squatting. But in case of cyber-crime like Hacking, Internet time thefts, Email bombing- there is nothing contained in our penal code. So it can be said that it is not possible for our government to control cybercrime by using some provision of the penal code. To controlled cybercrime it is necessary to enact special law which only deals with cyber related matters. The Government of Bangladesh passed Information Technology Act on 2006. This is the statute enacted by the government of Bangladesh with a view to consolidate Computer related matters. This statute contains several provisions regarding damage to computer and computer system. Cybercrime dictates that prohibits attacks or unauthorized access to computers and computer systems [13].

According to Section 66 of the ICT Act provides Punishment for tampering with computer source documents. Section 66 says whoever intentionally destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs or with both [13].

Section 67 Hacking with computer system. Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of “hacking”[13].

Section 68 of the ICT Act provides punishments for the hackers. Section 68 says that whoever commits hacking shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to taka two lakhs or with both. But the problem of this act is this act deals with so many things. The act is made to cover all the information technology related matters. But it is not possible to cover all the things by implementing just only one act. In order to control cyber-crime we need to have one specific cyber law in our country [13].

V. CONCLUSION AND RECOMMENDATIONS

Cybercrime a social disease is the global and universal phenomenon and it has no exclusive territory to be committed. As a result, the measure of preventing it should not be taken in isolation by any country. For this purpose, we should determine a universal definition of cybercrime which would be applicable for any state irrespective of geographical location. In the same way, the laws and policies should also be harmonized for prosecuting the criminals. No sovereign state the right to oblige any sovereign state to prosecute any criminal. Practically the criminals might not be the citizen of the affected country. As a result, the affected country should come forward to develop their laws and policies as well regulation to prosecute those criminals. Here, the national law might get priority over the international laws. Interestingly, it may not function if the extradition treaty has not been already made between the countries. Cybercrime having the trans-boundary nature, all states should cooperate to combat this crime. If any state does not function for fighting against this crime, the criminals may attack on each and every computer and technological achievement of the universe from the country creating habitats for the criminals. As a result, this country should come under the regulation. It is evident that preventing cybercrime requires bi-directional digging though the tunnels, each of the approaches has unique difficulties and benefits [23].

Technology in today‘s world is one of the fastest changing things, so are the patterns, motives, ways of committing IT-related crime. It is unfortunate that Bangladesh has had little success in combating modern cybercrime though legislative measures. ICT Act and Pornography Act can prevent some of the banal cybercrimes that are almost obsolete, but a complete fiasco to the more ominous crimes such as money laundering, online theft, credit card hacking, virtual child pornography, and online fraudulence by image deformation, piracy and plagiarism, stock exchange fraudulence and so on. It has neither entered into a global pact regarding cybercrime nor strengthened existing laws nor updated according to the necessity nor applied them effectively. IT sector is growing pretty haphazardly which may backfire in near future which can be easily predicted by the recent aggravation of the situation. Cybercrime is like population explosion, once out of control, possesses an extremely daunting task to control. It is high time; Bangladesh should ponder upon this grievous threat and lessen the gap between international effort and national effort accordingly [24].

From the above discussions certain recommendations are appended below for due consideration: Formulate a National Cyber Security Policy as well as establish an entity for overall coordinating and directing responsibility. Create awareness and build momentum. Conduct extensive media campaigns and other civic activities to build mass awareness on cyber-criminal activities. Initiate programs to educate everybody about their cyber right and also edify parents on how to filter harmful Internet contents. Initiate dialogs with the NGOs, donor organizations and corporate bodies for sharing government’s vision and tentative roadmap towards combating cybercrime. Encourage senior officials of the government and public organizations to learn basic operations of Internet with alertness for functioning independently. Enhance law enforcement’s capabilities for preventing and prosecuting cyber-attacks. Promulgate stringent laws towards the menace of cybercrime. Laws should create deterrence in the mind of criminals. Every effort should be made for international cooperation to enable the information sharing, reduce vulnerabilities, and deter malicious users. Create appropriate structures at all level with well-defined role and responsibilities so that human resources with adequate skills, knowledge and training are available to securely manage the information infrastructure. A national level agency may be created for sanitization of hardware, software and computer related gadgets specially used in sensitive organizations [1].

REFERENCES

[1] Ahmed DR. Zulfiquar, A Text Book On Cyber Law in Bangladesh

[2] D Rodney Ryder, Guide to Cyber Laws, 2nded. (Nagpur: Wadha & Company, 2005)

[3] R. K. Chaubey, An Introduction to Cyber Crime and Cyber Laws, 1sted., (Kolkata: Kamal Law House, 2009).

[4] Zulfiquar Ahmed, A Text Book on Cyber Law in Bangladesh, 1sted., (Dhaka: National Law Book Company, 2009).

[5] Cyber Law in Bangladesh (Information and communication Technology Act, 2006) Media, Press and Telecommunication Laws in Bangladesh.

[6] Media and Cyber Laws in Bangladesh (Telecommunication, print, Broadcast, Film and Online Media Law with commentary and case law)

[7] Digital Security Act 2016 (draft)

[8] Penal Code 1860

[9] Criminal Code of Procedure 1898

[10] The Computer Misuse Act (1990)

[11] The Computer Fraud and Abuse Act, 1984

[12] The Convention on Cyber Crime, 2001

[13] Information and Communication Technology Act (ICT), 2006.

[14] Burruss, George W., Bossler, Adam M. And Holt, Thomas J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. Crime and Delinquency, 59(5), 1157-1184

[15] Hinduja, Sameer and Kooi, Brandon. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. Security Journal, 26(4), 383-402

[16] Patchin, Justin W. and Hinduja, Sameer. (2011). Traditional and non-traditional bullying among youth: A test of general strain theory. Youth & Society, 43(2), 727-751.

[17] Reyns, Bradford W. (2013). Online routines and identity theft victimization: Further explaining routine activity theory beyond direct-control offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238

[18] Runions, Kevin C. (2013). Toward a conceptual model of motive and self-control in cyber-aggression: Rage, reward and recreation. Journal of Youth and Adolescence, 42(5), 751-771.

[19] Van Wilsem, Johan. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. European Journal of Criminology, 8(2), 115-127

[20] Dug gal Mr. Pavan,"Causes of Cyber", Intenational Journal of Computer Science and Information Security, Vol.3, No. 1(October, 2009).

[21] Biswas Ripon Kumar, „Cybercrimes need more attention," Tuesday, September 09, 2008

[22] M. Abul Hasanat, „Cyber Crime: An Ill-going Techno - Culture", Journal of Law, Vol. i, no.1 (June 2003).

[23] <[http://www.naavi.org/pati/pati_cybercrimes_dec03.htm>

[24] <http://www.slideshare.net/fakrulalam/bangladesh-cyber-security-status-in-

[25] <httpwww.bdlawdigest.orgcyber-crime-a-new-menace-in-modern-era>

[26] <http://www.risingbd.com/english/cyber-crime-in-bangladesh-a-growing-threat-in-digitalmarketplace/ 28940

[27] <http//www.progressbangladesh.com/maximum-14-tears-in-jail-for-cyber-crimes/>