**Focus Keyword**: Cyber Crimes and Cyber Laws in Bangladesh

In 1997, John Carlin wrote an article for the Wired Magazine titled *‘A Farewell to Arms’*. While Ernest Hemingway’s novel of the same name tells about a soldier literally bidding farewell to arms, John Carlin’s article presents a completely different scene. In his article John Carlin brought forth a new idea. What he meant to say is that future wars won’t require conventional weapons. Instead they will be fought in another way. The way he foresaw nearly two decades ago is the reality of today.

Today we often come across terms like ‘cyber crimes’, ‘net crimes’, ‘computer-fraud’, ‘cyber extortion’ etc. With the advent and advancement of internet, a new type of crime has developed. It is most commonly known as the cyber crimes. The term cyber generally means computer network or virtual reality. So, cyber crime can simply be defined as crime which involves cyberspace or computer network or a protected computer system. As our modern age is entirely dependent on network based facilities, a slight inconvenience on its part can cause a lot of problems. A single misplacement of information or a single wrong stroke on a keyboard button can literally cause great havoc and destruction. Though these technologies have empowered us to do a great deal of things, it has also put us in a vulnerable position. We have created these things but now we are sometimes helpless in front of our own creation. Honest mistakes may happen but some people are intentionally taking advantages of these weaknesses. What they are doing is called cyber crime. They become active in the cyberspace and then use trickeries and evil methods to materialize their malicious desires which are often very harmful to individuals and group of individuals. These cyber crimes are dangerous in nature and always pose serious threat to privacy at personal, public or national level.

**What exactly is cyber crime?**

Dr. Debarati Haldar and Dr. K. Jaishankar defined cyber crimes as such-

“Offences that are committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as internet (chat rooms, emails, notice boards or groups) and mobile phone (SMS/MMS).’’

Cyber criminals are most commonly known as hackers. The term “hacker” is now so overused that it has come to be applied to anyone who breaks into computer systems. But this is not entirely correct. There is a difference between hackers and crackers, although the term “cracker” has never caught on with general public.

Hackers are people who gain unauthorized access to computers or telecommunication systems, often just for the challenge of it. They think it as a challenge which they accept for fun. Some of the hackers even believe and vigorously claim that they are performing a service by exposing weaknesses and security flaws of various computer networks. These hackers are not interested in obtaining anything or have no motivation for financial gain. On the other hand crackers are people who illegally break into computer systems for financial gains, shut down hardware pirate software or alter or destroy data. They often engage in sabotaging the victim’s assets. The aforementioned hackers are colloquially called ‘white-hat hackers’ (who are not malicious) and those mentioned later are called ‘black-hat hackers’ (who are malicious).

**Types of cyber crimes**

There are many kinds of cyber crimes. Some of them are briefly mentioned below-

**Hacking**

It is an offence to hack a computer system which belongs to other individuals or organizations. Hacking puts the victim in a very vulnerable position as there are risks of exposing all the confidential information in a computer system. It is a punishable offence and the laws regarding hacking are quite strict.

**Cyber-defamation**

The internet can be used to spread misinformation just as easily as information. Websites can present false or defamatory information especially in forums and chat rooms, where users can post messages without verification by moderators. IT is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a world wide range.

**Cyber-extortion**

Cyber-extortionists create harmful soft-wares and often threat individuals or organizations. With those soft-wares they can cause serious damage to the threatened individuals or   organizations. They offer ‘protection’ in exchange of money otherwise they destroy or expose all financial and security information. These cyber-extortionists can be regarded as the new age cyber-mafias.

**E-mail bombing**

E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victims e-mail account (in case of an individual) crashing. This kind of things are done to harass someone purposefully.

**Cyber-terrorism**

The term cyber-terrorism was coined in the 1980s by Barry C. Collin. It is defined as the premeditated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Cyber-terrorists can do unimaginable harm to a group of people or a state. They can get into a telephone network during an emergency and shut it down causing more casualties. Suppose, a situation similar to 9/11 has arisen and emergency personnel are being deployed. Meanwhile, the terrorists can hack into emergency communication system and redirect all orders, give false information etc. Thus, the situation will worsen. In USA, FBI has separate Cyber Security Unit (CSU) who works to protect the nation from such attacks. Cyber-terrorists target transportation, telecommunication, financial data etc. Thus, a war can be won without shooting even a single bullet.

**Cyber-crimes in Bangladesh**

Bangladesh, despite being a third world country, has seen a technological revolution. A Bangladeshi teenager has very easy access to computers and other devices. And so, they get enough opportunity to engage in hacking. Hacking has already become a major problem in Bangladesh. Young people are getting more and more interested in hacking for the thrill in it. Not just young people, even the mainstream media is so often engaged in the hacking and exposing private information.

The Mahmudur Rahman case is one of the leading cases in terms of cyber crimes in Bangladesh and may be referred as the first cyber crime case in Bangladesh. Mahmudur Rahman, the founder of a Bangladeshi newspaper named Amar Desh was sued in line with a High Court directive for publishing reports on Skype conversation between former International Crimes Tribunal chairman Justice Md Nijamul Huq and an expatriate  legal expert in December, 2012. He was sued along with the Amar Desh publisher Hashmat Ali on December 13, 2012.

On 15/02/2012 a group of alleged Bangladeshi hackers  named ‘Black Hat Hackers’ hacked more than 25000 Indian websites which included important sites such as the website of the Border Security Forces (BSF). Propaganda activities are also considered as cyber-crimes in some instances. Propaganda is information which is biased and misleading in nature used to promote or publicize a particular political cause or ideology. It creates agitation and panic among the public. For example, we can mention the 2012 Ramu Violence in Cox’s Bazar. Someone with a fake Facebook account posted a photo of desecration of the Holy Quran on its wall. The fake account was under a Buddhist male name. This post agitated the common Muslim people of that area and they, without verifying the authenticity of the Facebook account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were destroyed. So, it is clear that Bangladesh is not free from the threat of cyber-crimes. Everyday new forms of cyber-crimes are happening and if it goes unchecked, law and order situation will worsen.

**Legal fabric of Bangladesh regarding cyber-crimes**

*The*[***Information and Communication Technology (ICT) Act, 2006***](http://bdlawdigest.org/wp-content/uploads/2015/08/ICTAct2006English.pdf) came in force on 8 October, 2006. Subsequently, the government amended the Act in 2008 and in 2009. For the better application of the Act, the government passed Information Technology (Certificate Authority) rules in 2010. But these laws alone are not enough. To face the challenges growing in cyber space it is essential to amend the existing laws such as *the Penal Code 1860*, *the Evidence Act 1872*, *the Contract Act 1872* etc. It is hoped that these Acts will be modified in accordance with the demand of time. However, there are some provisions in the ICT Act, 2006 which mention penalties for various cyberspace related crimes. For instance,*section 54 (1)* of this Act declares the offences concerning cyberspace. Then, *section-54(2)* says, “If any person commits offences under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka ten lakhs, or with both”.

We can also look at *section-56* which says-

“If any person—

       (a) with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any 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;

       (b) damage through illegal access to any such computer, computer network or any electronic system which do not belong to him; then such activity shall be treated as hacking offence;

    (c) whoever commits hacking offence under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka one crore , or with both.”

We can see that law has taken the matter of cyber-crimes in consideration and there are some strict rules regarding it.

**Conclusion**

Cyber crime is obviously the latest form of the crimes which is very difficult to suppress. But, its difficulty must not prevent us from taking adequate measures against the cyber-criminals. Only law is not enough and so, we must nurture ethics and morality in our private and communal lives. As our youngsters are prone to misdirection, they must be given proper guidance and care. The state has to take all possible measures to thwart any kind of cyber-invasion which may put the lives of people in danger. Continuous vigilance and upgrading counter-measures are some of the must-dos for the government. Common people should also be careful in using computer systems and online facilities. Hopefully, our awareness and constant battle against cyber-crime will result in success.

**Cite this article as:** Md. Sarwar Alam Sajjad, 'Cyber Crime and Legal Fabric of Bangladesh' (*Bangladesh Law Digest*, August 12, 2015) <<http://bdlawdigest.org/cyber-crimes-and-cyber-laws-in-bangladesh.html>>

**Copyright:** Any unauthorized use or reproduction of Bangladesh Law Digest (BDLD) content for commercial purposes is strictly prohibited and constitutes copyright infringement liable to legal action.