Cyber Crime, Law and Bangladesh Perspective

Cyber-crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading have led to a phenomenal spurt in incidents of cyber-crime. Cyber law is also known as Internet Law.

"Cyber law is a term used to describe the legal issues related to use of communication technology, particularly "cyberspace", i.e., the Internet. It is less a distinct field of law than property or contract as it is an intersection of many legal fields including intellectual property, privacy, freedom of expression and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legal system applicable to the visual world."

World Statistics:[1]

Victims per year	556 million
Victims per day	Over 1.5 million
Victims per second	18
Identities exposed	More than 232.4 million

More than 600,000 Facebook accounts are compromised every day.

15% of social network users have reported that their profiles have been hacked by pretenders.

1 in 10 social network users said they'd fallen victim to a scam or fake link on social network platforms.

Top 15 Countries Where Cyber Attacks Originate (February 2013):[2]

Source of Attack	Number of Attacks
Russia	2,402,722
Taiwan	907,102
Germany	780,425
Ukraine	566,531
Hungary	367,966
USA	355,341
Romania	350,948
Brazil	337,977
Italy	288,607
Australia	255,777
Argentina	185,720
China	168,146
Poland	162,235
Israel	143,943

[1] http://www.go-gulf.com/blog/cyber-crime/
[2] http://www.go-gulf.com/blog/cyber-crime/

Japan	133,908

Cyber-Crimes at a glance:

The common cyber-crimes all over the worlds are

- **Hacking** (unauthorized access to computer systems or networks)
- **Email bombing** (… refers to sending large numbers of mail to the victim….there by ultimately resulting into crashing).
- **Data diddling**(… an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed)
- **Salami Attacks** (demonstrated by the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account)
- **Denial of Service attack/Distributed Denial of Service (DDoS)** (When a user is illegitimately prevented from accessing a service such as Amazon or Yahoo)
- **Virus / worm attacks** (an example of this being the ""love bug virus, which affected at least 5 % of the computers of the globe)
- **Logic bombs** (some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date, like the Chernobyl virus),
- **Trojan attacks** (its origin in the word 'Trojan horse' as the unauthorized program is inside what appears to be an authorized application).

Cyber-Law: Bangladesh Perspective

In the Information and Communication Technology Act of Bangladesh does not define what the Cyber law by any section. But Cyber laws are contained in the Information and Communication Technology Act, 2006. Therefore this Act provides the legal infrastructure for e-commerce and other legal solutions relating with cyber-crimes in Bangladesh.

Cyber Crimes in ICT Act, 2006:

Chapter eight sections 54 to 67 of the ICT Act 2006 describe the Cyber Crimes both civil and criminal matters. The followings shall be treated as crime**;**

- Unauthorized copying, extracting and downloading of any data, database
- Introduction of virus
- Damage and disruption to computer system and computer network
- Denial of access to authorized person to computer
- Providing assistance to make possible to commit to crime
- Hacking with computer system
- Tampering computer source documents
- Electronic forger for the purpose of cheating and harming reputation
- Using a forged Electronic record
- Publication of digital signature certificate for the fraudulent purpose
- Confiscation of computer, network etc.
- Publication of information which is obscene in electronic form

- Misrepresentation and suppressing material facts for obtaining digital signature certificate
- Breachof confidentiality and privacy
- Publishing false digital signature certificate

Cyber Crimes Scenario in Bangladesh:[3]

Recently in Bangladesh, 4 students of a private technology institute hacked the RAB web site. On 23 June 2009 RAB arrested JMB IT chief Rajib who used the internet as an engine of resources to make explosives to use in terrorism activities as he confessed that "I download information on explosives from internet, translate those in Bengali and send those to Mizan through Bashar[4]". This is a serious concern for our national security.

In 2008 a petty hacker of Bangladesh named Shahi Mirza hacked the RAB's website. Moreover he confessed to police that not only RAB's website but also other national govt. and non govt. and international site had been hacked by him for a long time. Totally he hacked 21 website together with Army's website.[5] So it is clear to us that the cyberspace of Bangladesh is not secured.

Penalty or Punishment under the ICT Act, 2006:

- If any person does any crime under section 54 of the ICT Act 2006 he will be given penalty of maximum 10 years rigorous imprisonment or fined up to 10 lacs taka or for the both of above.
- If any person does any crime under section 55 he will be given penalty of maximum 3years imprisonment or fined up to 3 lacs taka or with both. Whoever commits hacking under this act shall be punished of maximum 3 years imprisonment or fined up to 1 crore taka or with both.
- Whoever commits such crime under section 57 (uploading vulgar and obscene contents on website) of this act shall be punished of maximum 10 years imprisonment or fined up to 1 crore taka or with both.
- Penalty for failure to surrender license is 6 month imprisonment or fined up to 10 thousand taka or with both.
- Penalty for failure to comply with order made by the controller is maximum 1 year's imprisonment or fined up to 1 lacs taka or with both.
- Penalty for violation of the order of the controller in emergency period is maximum 5 years or fined up to 5 lacs or with both.
- Punishment for unauthorized access to protected system is the maximum 10 years or fined up to 10 lacs or with both.
- Penalty for false representation and hiding information is maximum 2 years imprisonment or fined up to 2 lacs or with both.
- Penalty for discloser of confidentiality and privacy is maximum 2 years imprisonment or fined up to 2 lacs or with both.
- Punishment for publishing false digital signature certificate is maximum 2 years imprisonment or fined up to 2 lacs or with both.
- Penalty for Publication of digital signature certificate for the fraudulent purpose is maximum 2 years imprisonment or fined up to 2 lacs or with both.

[3] The Daily Star,Friday,07 February, 2014

Weakness of the ICT Act, 2006:

The ICT Act has some specific weakness. The law does sometimes regulate the social norm and then control of information technology. We can discuss about the few weakness of the Act. ICT Act 2006 does not define the definition of "Cyber law". Subsequently the law does not give proper solutions about the Intellectual Property Right and this law does not discuss of about the rights and liability of domain name holders. Experts think that it is the first step of entering into the e-commerce. Not only these weaknesses of the Act but also others problems can to be brought through the Act.

Recommendations:

- Strengthening cyber law;
- Immediately amend the weakness and problems of ICT Act 2006;
- Cooperation, sharing of knowledge and practical experience;
- Internet users need awareness about cyber-crime;
- Do not use internet in cyber café;
- Government should ensure law;
- Immediately need punishment against cyber-crime;
- Independence of cyber tribunals;
- Government should establish more cyber tribunals;
- Establishment of a free cyber commission;
- Establishment of digital forensic laboratory for investigation and detection of cyber-crime;
- Promotion of standardization of methods;
- Establish good practice guidelines;
- To share the current crime scenes;
- To train trainers or teachers on IT crime investigation;
- Usage of Interpol Criminal Information System and Interpol Secure Web Site https://www.interpol.int;
- Effective usage of National Central Reference Points;
- To initiate IT related projects;
- Finally cyber law should be included in the syllabus of our legal system.

Now a day, cyber-crime has become as a burning question. Present government always desires to be digitalized. To make digital Bangladesh, government should immediately amend ICT Act and to take proper steps for more security. For prosperous Bangladesh, we always should be aware about cyber-crime and law.

Written by:

Md. Ramim Hassan

Session: 2011-2012

Dept. Of Law

Islamic University

Kushtia.