Cyber law: Bangladesh perspective

BY:
MD AMRAN HOSSAIN
EMCS, JAHANGIRNAGAR UNIVERSITY

Introduction:

Global economic strength depends on strong communication infrastructure. Being a part of global economy Bangladesh has to adopt up-to-date digital infrastructure to continue its information relationship with rest of the world, who already have adopted the necessary technologies and have been facing unique challenges every day. Developed countries have already transformed their financial, economic, agriculture, health, telecommunications, common utilities, education, and public safety sectors into hi tech digital technologies. Though we are in an initial stage of this D-tech; once we successfully apply it we will certainly face the mentioned critical situations that are being suffered globally.

What is Cyber Law?

“Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law than property or contract are 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 legacy system of laws applicable to the physical world.”

Why Cyber Law?

To control the misuse of the technologies in order to protect nations/states and bring the criminals within the jurisdiction, an effective cyber law can play a vital role in ensuring that national and global criminals are fairly and successfully tried and judged for their crimes.

Cyber crimes:

- **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 Crimes use computers and networks for criminal activities. Computers can be used for committing a crime in one of the following three ways

- As a tool
- As a target
- Both as a tool and a target

A partial list of cyber crimes are as follows;

- Hacking of computer systems and networks
- Cyber pornography involving production and distribution of pornographic material, including child pornography
- Financial crimes such as siphoning of money from banks, credit card frauds, money laundering
- Online Gambling
- Intellectual property crimes such as theft of computer source code, software piracy, copyright infringement, trademark violations
- Harassments such as cyber stalking, cyber defamation, indecent and abusing mails
- Cyber frauds such as forgery of documents including currency and any other documents
- Launching of virus, worms and Trojans
- Denial-of-service attacks
- Cyber attacks and cyber terrorism
- Economic espionage
- Consumer harassment and consumer protection
- Privacy of citizens
- Sale of illegal articles such as narcotics, weapons, wildlife, etc

Cyber crimes that can generally occur within organizations are as follows

- E-mail abuse
- Spam mails
- Cyber defamation
- Theft of source code
- Exchange of business secrets and documents
- Insider attacks on personal database
- Use of office computer for running other business
- Transmission and viewing of pornographic materials

- External cyber attacks on an organization resulting in denial-of-service
- Information espionage

Scenario:

American election properties have been stolen by the cyber intruders worth 400 million dollars. In June 2007 intruders hacked pentagon network. 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 (The Daily Star)," which 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. So it is clear to us that the cyberspace of Bangladesh is not secured.

Few months ago Bangladesh government imposed restriction on opening you- tube video site because it contains an audio recording of a March 1 encounter between angry army officers and the prime minister. The recording was made on March 1 during an emotional meeting at the Dhaka cantonment. Hundreds of officers were present, distraught after paramilitary soldiers brutally killed more than 50 members of the army, including many of the leaders of the Bangladesh Rifles border force. Bangladesh government says in front of media that you-tube has been blocked in the interest of national security.

In September 2007, most internet service providers (ISPs) in Bangladesh were affected by the Denial of Service (DoS) attack. A large volume of data packets was transmitted from an American data centre and caused server failure, slowing the performance of almost all ISPs. The attack was initially attempted on one ISP, Global Access Limited (GAL). Such attack causes serious damage. But our government remains silent after the attack and said in front of media that we have nothing to do.

Cyber Act 2006:

To define and amend certain parts of law relating to legal recognition and security of information and communication technology and related matters the Information and Communication Technology Act-2006 was enacted. According to the ICT Act the cybercrime shall be treated as non cognizable offence that is why the police can't arrest the criminals without warrant except some cases.

Chapter eight section 54 to 67 of the ICT Act 2006 describe the cybercrimes 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
- Breach of confidentiality and privacy
- Publishing false digital signature certificate

Penalty or punishment:

- 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.

Issues on Cyber Act 2006:

The Information Technology Act 2006 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

1. **The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose**. Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

2. "**Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime**" – Mr. Pavan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the ICT Act 2006 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime.

3. **Cyber torts**- The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the ICT Act 2006 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the ICT Act 2006 read with the Penal Code is capable of dealing with these felonies.

4. "**Cyber crime in the Act is neither comprehensive nor exhaustive**"- Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- "The IT Act, 2006 is not comprehensive enough and doesn't even define the term 'cyber crime". Mr. Duggal has further commented, "India, as a nation, has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes."

5. **Ambiguity in the definitions**- The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The infamous "go2nextjob" has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the netizens are till s. 66 exists in its present form. Further section 67 is also vague to certain extent. It is difficult to define the term *lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by "the Bal Bharati case".

6. **Uniform law**- Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

7. **Lack of awareness**- One important reason that the Act of 2006 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court

in October 2002 prevented a person from selling *Microsoft pirated software*over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for "online cheating" by buying Sony products using a stolen credit card.

8. **Jurisdiction issues**- Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2006 is very silent on these issues.

9. **Extra territorial application**- Though S.4 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

10. **Raising a cyber army**- By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the "Cyber Crime Investigation Cell (CCIC of the Central Bureau of Investigation (CBI 11 " is definitely a welcome step in this direction. There are man cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –

- Case 1: When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

  Status: Probe on

- Case 2: CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.

  Status: Charge sheet not filed

- Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

  Status: Pak not cooperating.

11. **Cyber savvy bench**- Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. Mr T.K.Vishwanathan, member secretary, Law Commission, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated "if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System".

12. **Dynamic form of cyber crime**- Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, “In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind.” The (de-creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

13. **Hesitation to report offences**- As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the "Delhi time theft case". “The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business.” This attitude of the administration is also reveled by incident that took place at "Merrut and Belgam". (for the facts of these incidents refer to naavi.com. For complete realization of the provisions of this Act a cooperative police force is require.

14. **Time limitation**- Chapter eight of the ICT Act creates a cyber tribunal to adjudicate of cybercrimes. The judge of the tribunal will complete the judgment procedure within 6 month of filing the case. The judgment will be given within 10 days from the date of finishing examination of witness or evidence or hearing.

Conclusion:

The policy maker may formulate a baseline security procedures policy outlining the minimum requirements which must be met by agencies regarding information security and may also develop a special analysis site which will be observed 24/7 and will provide real-time monitoring of cyber activities. ‘Cyber incident response unit’ and ‘a cyber crime investigation cell’ may be built within law enforcement authority to fight cyber crime successfully by adopting the enhancing ‘capacity’, good police work, skilled investigators by sharing the ‘too few’ professionals skilled in cyber-security and by training new officers to become experts in the field and providing adequate logistic support/equipment.

Moreover, to keep the national security uninterrupted and avoid hacking, web servers running public sites must be physically separate protected from internal corporate network and web site owners should watch traffic and check any inconsistency on the site by installing host-based intrusion detection devices on servers.

Finally, we can say that the collective effort of state and nations is only a possible way to see the peoples’ dream of a Digital Bangladesh in existence and could protect individuals and national security of the state from the aggression of cyber criminals.