International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-3, Issue-5, May 2017 Pages 01-06

Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law

Dr Mir Mohammad Azad, Kazi Nafiul Mazid, Syeda Shajia Sharmin

***Abstract*— Cyber crime, or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Debarati Halder and K. Jaishankar define 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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".**
Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

***Index Terms*— Cyber Crime, Cyber Crime legal areas, Cyber Crime Law.**

I. Introduction

Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individuals private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files. Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. A report (sponsored by McAfee) estimates that the annual damage to the global economy is at $445 billion; However, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude.[third-party source needed] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019.

Dr Mir Mohammad Azad, Department of CSE and CSIT, Shanto Mariam Unniversity of Creative Technology, Dhaka, Bangladesh

Kazi Nafiul Mazid , Department of LAW, Shanto Mariam Unniversity of Creative Technology, Dhaka, Bangladesh,

Syeda Shajia Sharmin, Department of LAW, Shanto Mariam Unniversity of Creative Technology, Dhaka, Bangladesh

II. Problem Areas

1. Telecommunications
2. Electronic vandalism, terrorism and extortion
3. Stealing telecommunications services
4. Telecommunications piracy
5. Pornography and other offensive material
6. Telemarketing fraud
7. Electronic fund transfer crime

III. Legal Areas

Here are just a few rhetorical questions about the law relating to search and seizure of electronic evidence. These were formulated in October 1998 at a special expert working group meeting convened in Tokyo under the auspices of the United Nations and with the involvement of the Australian Institute of Criminology.

A. Investigative Issues

(i) Does the law distinguish between the search and seizure of stored data in a computer, and the interception of data that is being communicated from one computer to another or within a computer system?

(ii) Can a person voluntarily provide law enforcement agents with electronic data that may afford evidence of a crime? Can a person voluntarily permit law enforcement agents to undertake a search for such data, rather than provide it to them? Could continuing cooperation of this nature by a person with law enforcement have a legal effect on the ability of law enforcement to obtain or use the data?

(iii) In most jurisdictions, the ability of law enforcement to obtain data that may afford evidence usually requires some form of prior judicial approval. What legal authority is required for obtaining electronic stored data without the consent of the persons concerned?

(iv) Electronic data under most jurisdictions is considered as being intangible. The law of some jurisdictions may only permit seizure of tangible material. In such cases, intangible data can only be obtained by seizing the physical medium (e.g., data on diskette or other storage medium) on which the

data is stored and found. Do your nation's laws provide for the seizure of intangible data without seizure of the physical medium which it is found?

(v) In some cases, the precise location of electronic data within a computer system may not be apparent. How specific must be the description in the judicial authority (e.g., search warrant) of the place to be searched or the data to be seized?

(vi) In most jurisdictions, the scope of a warrant should be as narrow as possible. The precise location of the electronic data may not be immediately apparent at the time a warrant is sought, or even when law enforcement agents arrive at the scene. Does the law provide guidance on whether to seize the entire computer system, or merely one or more of its components? What practical criteria do law enforcement use to make this decision? How would this be done in practice?

(vii) Does your law obligate a suspect or a third person to provide access (including passwords) to a computer system that is the target of a lawful search? If not, what practical measures or tools can be employed by law enforcement to gain access?

(viii) Seizure of, or during the course of a search the shutting down of, an entire computer system may be extremely intrusive, and particularly burdensome to an ongoing business. What practical circumstances would justify seizing or shutting down a complete system rather than merely taking a copy of the data? Does the law provide for copying of relevant data as an alternative to seizure, and can the copy be regarded as admissible evidence? Would the law permit the seizure of the entire data base for the purpose of subsequently identifying the relevant data? What practical means can be used to copy large volumes of data?

(ix) In the course of a search, law enforcement authorities may come across incriminating data related to the crime under investigation, but which was not originally specified within the scope of the warrant. Can this data be legally seized without obtaining another warrant?

(x) In the course of a search, law enforcement authorities may come across electronic data relating to a crime different from that which is under the current investigation. Can this data be legally seized without obtaining another warrant?

(xi) Does the law permit seizure of data, without a warrant, under exigent circumstances, such as when there is risk of erasure or destruction of data? Alternatively, are law enforcement agents able to secure the premises or computer system, pending the obtaining of a warrant?

(xii) In some cases, the data sought may be located on another computer system that is networked to the system currently being searched. Does the law permit an extension of the search into the connected system in order to search and seize relevant data within the scope of the warrant? Can the warrant include an authorization to extend the search to the connected system? Alternatively, can law enforcement obtain a second warrant to extend the search from one system to the other?

(xiii) Are there any circumstances under which the law permits stored data to be obtained by means of a judicial order to deliver such data to law enforcement authorities, as opposed to the law enforcement authorities themselves searching and seizing it?

B. Stored Transaction Data

(i) Records of service use, also known as transaction data, may be kept by some telecommunication carriers and internet service providers. Some carriers or ISPs may, for business or security purposes, retain such data for a period of time. In some jurisdictions, the cooperation of Internet service providers (ISPs) in identifying suspects may be obtained informally. Can this data be voluntarily provided to law enforcement agents by carriers and service providers? Does the law provide a means by which this data can be compulsorily obtained by law enforcement authorities?

(ii) Which types of transaction data does law enforcement require? Which types of transaction data do telecommunications carriers retain? For how long do the carriers or ISPs retain such data? Are there any laws or regulations which require them to retain such data, or to dispose of it after a certain period of time?

C. Electronic Communications

(i) Does the law permit law enforcement to collect current or future transaction data (including the source or destination of communications)? Can this authority for collection of current and future transaction data be achieved by satisfying legal conditions less onerous than that required to intercept the content of communications? What practical or technological means can be used to collect such data? Does law enforcement have the capability to undertake such techniques?

(ii) Even when one is able to determine the location from which a communication originates, identifying the human source of the communication may prove to be challenging. What legal and/or technological tools are available for this purpose?

(iii) How is the ability to collect such current or future transaction data affected if the communication crosses jurisdictional borders, including international borders?

(iv) Does the law permit interception of communications for the purpose of obtaining their content? Does the law permit this interception in respect of communications between computer systems or their components, as well as between persons? Does law enforcement have the practical capability to undertake such investigative techniques?

(v) In some cases, search or interception may be more efficiently and more effectively carried out by representatives of the telecommunications or ISP industry rather than law enforcement personnel. Does the law provide authority or obligation for private organizations or individuals to engage or assist in interception or search on behalf of the state? How does this affect the admissibility of the data as evidence in judicial proceedings? If there is no such authority or

obligation, are there trained law enforcement personnel to undertake this task, and how would they do so?

D. Analysis of Data

(i) What legal, practical or technical means are available to preserve the data seized or intercepted in order to ensure its presentation and admissibility in judicial proceedings? What procedures should be followed?

(ii) If the data seized are encrypted, what legal, practical or technical means are available to allow law enforcement to decrypt data? Does law enforcement have legal authority to decrypt seized data using technical means? Can an order be sought from a judicial authority to compel decryption by the suspect or a third person? Can an order be sought to compel a suspect or a third person to hand over the encryption key or algorithm to law enforcement?

E. Human Rights and Privacy Safeguards

(i) Can a person to whom compulsory measures are applied, as above, challenge the lawfulness of such measures before a court, either before or after execution?

(ii) What legal protections exist for law enforcement agents who are undertaking a coercive investigative measure such as a search and seizure, or interception?

(iii) Which types of remedies may be ordered by a judicial authority?

(iv) How would such remedies be obtained or enforced in the context of a trans-border search?

(v) To what extent would legal protections or immunities apply to law enforcement from another country who are undertaking a trans-border search in your country?

IV. The Cyber Law and Penalties

It aims to address legal issues concerning online interactions and the Internet in the Philippines. Among the **cybercrime** offenses included in the bill are cyber squatting, cybersex, child pornography, identity theft, illegal access to data and libel. Internet has become the backbone of all kinds of communication systems and it is also one of the most important sources of knowledge in the present digitalized world. It is a network of networks that consists of millions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber optic cables, wireless connections, and other technologies.

Definition of cyber crime: The degree of overlap between organized crime and cybercrime is likely to increase considerably in the next few years. This is something that needs to be recognized by business and government as an emerging and very serious threat to cyber-security. Cyber crime can broadly be defined as a criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception, data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), and systems interference, misuse of devices, forgery (theft), and electronic fraud. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber crime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. In short, it is unlawful acts wherein the computer is either a tool or a target or both. Types of Cyber Crimes: When any crime is committed over the Internet it is referred to as a cyber crime.

There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Currently, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, social security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history. Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system. Cyber Defamation: This occurs when defamation takes place with the help of computers and or the Internet e.g. someone publishes defamatory matter(s) about someone on websites or sends e-mail to his friends containing defamatory information.

E-mail spoofing: A spoofed email is that email which appears to originate from one source but actually has been sent from another source. This can also be termed as e-mail forging. Child soliciting and abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the

purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting. Bangladesh has by now already become a victim of cyber crime. The incident of Bangladesh bank heist is one of the proven evidences. Legal response to cyber crime in Bangladesh In order to facilitate e-commerce and encourage the growth of information technology, the Information and Communication Technology (ICT) Act, 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or both. However, recently the National Parliament amended the ICT Act 2006. The cabinet approved the draft of the ICT (Amendment) Act-2013 on August 19 proposing to empower law enforcers to arrest any person without warrant and increase the highest punishment to 14 years from minimum 7 years or a fine of Tk. 1 crore or both. The bill made offences under sections 54, 56, 57 and 61 of the ICT Act, 2006 cognizable and non-bail able, empowering law enforcers to arrest anyone accused of violating the law without a warrant, by invoking section 54 of the Code of Criminal Procedure. All such offences were non-cognizable in the ICT Act, 2006. However, all concerned apprehend of the misuse of the power by the police. The ICT Act, 2006 as amended in 2013 is obviously a brilliant achievement of Bangladesh in the field of cyber law.

Critics point out that still there remain certain specific limitations of the said Act as under:

(1)The Act remains silent about various intellectual property rights like copy right, trade mark and patent right of e-information and data.

(2) The enactment has a major effect on e-commerce and m-commerce in Bangladesh. But it keeps itself mum as to the electronic payment of any transaction.

(3) The legislation was initially supposed to be applied to crimes committed all over the world; but nobody knows how this can be achieved in practice.

(4) Spamming has become a peril in the West as such they have made anti spamming provisions in cyber law. However, there is no anti-spamming provision in our Act.

(5) Domain name is the major issue which relates to the internet world thoroughly. But the ICT Act, 2006 does not define 'domain name' and the rights and liabilities relating to this.

(6) The Act does not address any crime committed through using mobile phones.

(7) This law made e-mails as evidence, conflicting with the country's Evidence Act that does not recognize e-mails as evidence.

A session judge or an additional session judge will preside over the Cyber Tribunal and a bench of three members including a chairman who will be an ex or acting judge or a competent person to be a judge of Supreme Court and an ex or acting Dist. Judge and an ICT expert, two other members of the bench, will preside over the Cyber Appellate Tri bunal and like the other criminal cases Public Prosecutors will prosecute on behalf of the state in this regard. The problem is that judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes.

International perspective on cyber crime: Cyber crime is becoming ever more serious. Findings from Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. Each state are reacting to the need of cyber laws. As expressed below-USA - The United States, to protect the interests of internet businesses, the US Congress has enacted new laws to regulate activities on the internet. With the first digital signature law in the world, the US has established a number of regulations on cybercrime, such as the "National Infrastructure Protection Act of 1996", the "Cyberspace Electronic Security Act of 1999" and the "Patriot Act of 2001". In addition a number of agencies have been set up in the US to fight against cybercrime, including the FBI, National Infrastructure Protection Center, National White Collar Center, Computer Hacking and Intellectual Property Unit and so on. The FBI has set up special technical units and developed Carnivore. England - Two cyber crimes related Acts have been passed by the British Parliament the Data Protection Act of 1984 and the Computer Misuse Act of 1990. The former one deals with actual procurement and use of personal data while the latter defines the laws, procedures and penalties surrounding unauthorized entry into computers. The British government has applied technologies of filtering and rating to protect manors from inappropriate material on the Web. Canada - in 2001, the Canadian Parliament passed the Criminal Law Amendment Act that has two sections. The first section defines unlawful entry into a computer system and interception of transmissions. The second section criminalizes the actual destruction, alteration, or interruption of data. Norway - In Norway a Bill on a new Criminal Law (2008-2009) has introduced a provision on identity theft, using the term Identity Infringements that reads as follows:"With a fine or imprisonment not exceeding 2 years shall whoever be punished, that without authority possesses of a means of identity of another, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of a) procuring an economic benefit for oneself or for another person, or b) causing a loss of property or inconvenience to another person." India - The Indian Government has in 2003 announced plans on a comprehensive law for cybercrimes.

(i) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commit shack. (ii) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. The estimated number of internet users in the early years of the twenty-first century is over a billion. In this global village, consumers,

companies, and governments from around the world must further develop ways to protect the sensitive personal and business information and detect those, whether here or abroad, that conspire to exploit technology for criminal gain. Most of the developing countries like Bangladesh have limitations in access to information and the available access is not affordable because of the inadequacy of the existing infrastructure as well as the non-availability of appropriate education. The challenges are posed by the lack of an integrated computer security system and education about computer security. Therefore, there is a need for co-operation; collaboration and investment for security, which also develop the culture of security needs for assuring the security issue. The BTRC has to play a strong role in curbing cyber crimes as people of the country are in favor of bringing cyber criminals to book before they commit crimes like serial bombing, smuggling out national resources and extortion. Bangladesh Government should established one strong cyber police force squad. It is the duty of the government to provide security to all the citizens

V. Conclusion

Cyber crime is increasing day by day but our government is trying to protect. Every citizen should also be very careful about it. As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. According to the FBI's Internet Crime Complaint Center in 2014 there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073. [Citation needed] But yet cyber-crime doesn't seem to be on the average person's radar. There are 1.5 million cyber-attacks annually that mean that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.

References

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[2] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

[3] Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22, 2016.

[4] "We talked to the opportunist imitator behind Silk Road 3.0". 2014-11-07. Retrieved 2016-10-04.

[5] a b c Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.

[6] David Mann And Mike Sutton (2011-11-06). ">>Netcrime". Bjc.oxfordjournals.org. Retrieved 2011-11-10.

[7] "A walk on the dark side". The Economist. 2007-09-30.

[8] "DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children". Dhs.gov. Retrieved 2011-11-10.

[9] DAVID K. LI (January 17, 2012). "Zappos cyber attack". New York Post.

[10] Salvador Rodriguez (June 6, 2012). "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen". Los Angeles Times.

[11] Rick Rothacker (Oct 12, 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO". Reuters.

[12] "AP Twitter Hack Falsely Claims Explosions at White House". Samantha Murphy. April 23, 2013. Retrieved April 23, 2013.

[13] "Fake Tweet Erasing $136 Billion Shows Markets Need Humans". Bloomberg. April 23, 2013. Retrieved April 23, 2013.

[14] Richet, Jean-Loup (2013). "From Young Hackers to Crackers". International Journal of Technology and Human Interaction. 9 (1).

[15] Richet, Jean-Loup (2011). "Adoption of deviant behavior and cybercrime 'Know how' diffusion". York Deviancy Conference.

[16] Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry into Cybercrime." 17th AIM Symposium.

[17] Kshetri, Nir. "Diffusion and Effects of Cyber Crime in Developing Countries".

[18] Northam, Jackie. "U.S. Creates First Sanctions Program Against Cybercriminals"

Author's Profile

Dr Mir Mohammad Azad was born in Village – Korer Betka; Post Office – Mirrer Betka; Police Station - Tangail; District - Tangail, Bangladesh on 10th October, 1982.He received PhD in Computer Science, 2008 from Golden State University, Master of Computer Application, 2006 from Bharath Institute of Higher Education and Research Deemed University (Bharath University) and Bachelor of Computer Application, 2004, Bangalore University, India. He is pursuing **Bachelor of Law (LL.B) from National University of Bangladesh**. He was working as a **lecturer** and **head of computer science** in various colleges in Bangalore and also worked as an **Assistant professor** and **Vice Principal** in different colleges in Bangalore during the year (2005-2009).He worked as an **Assistant Professor** and **Head of CSE & CSIT** at **Shanto Mariam university of Creative Technology (2010-2014).** He is having **20** publications in international journal in various countries like UK, USA, FRANCE, KOREA, PAKISTAN, INDIA, GERMAN, and JAPAN. At present he is working as an **Associate Professor**, Department of **Computer Science and Engineering,** Department **Computer Science and Information Technology** in **Shanto Mariam university of Creative Technology**, Uttara, Dhaka, Bangladesh**.** His areas of interest include Computer Architecture, E-commerce, Digital Image processing, Computer Network, Wireless communication, MIS and Law.

Advocate Kazi Nafiul Mazid was born in Bagmara 2nd Lane, Khulna, Bangladesh on 20th August, 1971. He passed hisS.S.C. and H.S.C. respectively from Secondary and Higher Secondary Education Board, Jessore.He has completed hisB.S.S. and M.S.S. under National University. He also completed his M.B.A. from Royal Roads University, Canada. He has completedBachelor of Laws (LL.B.) andMaster of Laws. He has been awarded Chancellor's Gold Medal in his Master of Laws (LL.M.). Subsequently he has been enrolled with Dhaka Bar Association in 2006 and with Supreme Court Bar Association in 2008. He is a prominent practitioner in the Supreme Court of Bangladesh (Room No.-807-7th Floor, Annex Extension Building, Supreme Court Bar Association, Dhaka). Beside that he is the adjunct faculty in Southeast University and Northern University Bangladesh at the Department of Law.Also he is an Advisor at the Department of Law in Shanto-Mariam University of Creative Technology, Bangladesh. His areas of interest serve the nation in various law fields

Syeda Shajia Sharmin was born in Village: Khashipur,Post office: Daulatpur, Police Station: Khalishpur, District: Khulna, Bangladesh on 09 December, 1983. She passed her childhood in the city of Khulna as well as she achieved her Secondary School Certificate (S.S.C) and Higher Secondary School Certificate (H.S.C) respectively from Rotary School and Khulna Govt. Girls College,Khulna, Educational Board Jessore,Bangladesh. She has obtained Bachelor of Laws LL.B (Hon's)in the year of 2004 andMaster of Laws (LL.M) in the year of 2005 from University of Rajshahi, Bangladesh. She practiced as an Advocate at Dhaka Judges Court from 01-06-2006 to 31-03-2008 and also worked as a Lecturer of Department of Law, DarulIhsan University, 9/A Dhanmondi, Dhaka, Bangladesh from 21-04-2008 to 31-10-2013.She is also enlisted as an Advocate of Bangladesh Supreme Court in the year of 2014. At present she is working as a Lecturer of Law Department, Shanto-Mariam University of Creative Technology, Bangladesh. Her arenas of interests include as a subject and object in Law and Law related premises.