The Reality of Cyber Security in Bangladesh, Relevant Laws, Drawbacks and Challenges

Kudrat-E-Khuda Babu

Abstract Protection of data has become a matter of great concern as cyber-crime has now emerged as a major threat amid the rapid spread of the internet and information and communication technology across the globe. Despite being the most technologically advanced country, the United States is not out of the purview of the danger of cyber-crime. In such a situation, a country like Bangladesh which is still in the group of less developed countries is one of the most vulnerable countries in terms of cyber security. The Bangladesh government has gone through a huge digital transformation over the years and has been trying to connect the dots between the institutions digitally with the slogan of "Digital Bangladesh". Apart from that, national and multinational companies, operating in the country, are also offering online services to be part of the government's journey to the digital world. The distance between a consumer and a shop or a bank is now a click away, thanks to the wide access to the internet and the digital presence of the entities. Taking the advantage of easy excess and widespread use of the internet, opportunists and criminals have chosen the digital path to materialize their evil wishes. They are committing various crimes, including stealing money, and personal data, spreading rumors and cyber-attacks and other criminal activities. Amid the fragile security system, there is also a huge risk of targeted cyber-attacks by the hackers of any opponent country or frustrated group. Against this backdrop, it is evident that the state of cyber security in the country is very fragile and the existing laws and the measures of the state are very insignificant to tackle the growing threat. This study pinpoints the escalating cyber security concerns in the context of Bangladesh from a global perspective.

Keywords Bangladesh · Cyber security · Cybercrimes · ICT Act, 2006 · Digital Security Act, 2018

K.-E.-K. Babu (✉)
Department of Law, Daffodil International University, Dhaka, Bangladesh
e-mail: kekbabu.law@diu.edu.bd

H. Jahankhani (ed.), *Cybersecurity in the Age of Smart Societies*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-20160-8_6

1 Introduction

This is the high time for a revolution in information and communication technology in this age of globalization. Thanks to the rapid growth of technology, especially for the evolving information, and communication tools, now safeguarding cyberspace has become a crucial part of national security in the era of globalization. This is crucial for achieving economic stability and effective security in a country [17]. Information is saved, exchanged, and revealed in cyberspace, which is a realm of computer networks and the humans that use them [14]. Along with the transformation of the world into digital, the crimes of the actual world have also been shifted to the virtual with the same pace of the digital transformation. Once robbers looted a bank; now the virtual robber is heisting money from the bank by hacking their digital finance system. The cyber heist of $ 101 million from Bangladesh Bank reserve in 2016 has now become an old example of cybercrimes. So, there is no doubt that cyber-crime has become a foremost security issue for any state or organisation. Such crimes may be conducted by any individual or sometimes they may be unleashed by any state. The major concern is now the protection of confidential data. Posing a serious threat to the economic progress and defence systems, cybercrimes have become a cause of concern and escalated tensions in the diplomatic arena and eventually led to anarchy and even war in the world. Both misuses of information communication technology are now a major threat to global peace, stability, and development. As there is no strong surveillance system and security tools and measures, criminals can choose Bangladesh as a haven for committing crimes, including hacking and stealing personal data. Cybercriminals usually target digital services providers—both the government and non-state organisations—and steal personal and organizational data. In most cases, effective security steps are not taken at the time of providing digital services. As a legal security measure, the government enacted the Information Communication Technology Act (ICT Act), 2006 but it has failed to ensure cyber security due to a lack of proper use of the law. This study tries to identify the challenges for ensuring security in cyberspace in Bangladesh and shed light on the measures taken to check the cybercrimes from a global perspective. It also has scrutinized the current state legal frameworks, use and effectiveness to ensure efficient cyber security in the country. The final point of this study is that this is the prime time for Bangladesh to take strong measures to keep cyberspace safe and secure.

2 Cyber Security in the Global Village

Thanks to the evolution of information and communication technology, now people are very much connected globally and now they can commute from one edge to another edge of the world like a neighbour. And at a time, they can be connected from multiple parts of the globe within seconds. As a result, a new term has emerged among the global citizens called “netizens” and they have now made the world like

a village. Here comes the term global village. But despite the revolutionary changes in the cyber-world and security concerns for the netizens as well, the cyber threats have not gotten priority in the national security issues as well as the global concern. Not only are the netizens being victimised by the cybercrimes, but it also affects the state and even the globe too. As the most amount of money that is transacted daily in the world, through the digital transactions, cybercriminals always try to find the loopholes in financial networks and systems to extort money. According to Williams, there are four types of cyber-crimes, according to Williams. To begin with, cybercriminals are only interested in making money. In April 2013, for example, the US stock market lost $130 billion in minutes as a result of a hacked Twitter news stream spreading a bogus tale about an explosion at the White House [17]. Second, in their quest for sensitive knowledge or intellectual property, competing groups prey on one another. Both the civil and security businesses are concerned about this. A Russian criminal gang has amassed the largest known collection of stolen Internet data, which included 1.2 billion usernames and password combinations for over 500 million email addresses [13]. Thirdly, a de facto insider also appears as a threat sometimes. The incident of breaching the IT system of Iran's nuclear project and the leak of American diplomatic cables showed the vulnerability of the current system and stressed the need for ensuring cyber-security. However, the damage and losses for the cybercrimes are not proportional globally but the crimes have become more exacerbating due to the weakness in the security system in the cyberspaces.

Usually, cyber-crime predicts inevitable conflicts that will arise from close contact between different cultural practices through the internet. The revolution of information and communication technology has created people to people networks across the globe, connecting their organizational levels. Earlier, the communication process at the intra-organizational and governmental levels was so slow and expensive but the easy availability of the internet has changed the whole process of connectivity to an unparalleled level in terms of cost, speed and easy medium. Even for the sake of some software, it has also become so easy to send any information to a destination where there is no network for information transmission. Though this is helpful the users have to spend for it. However, amid the frequency of cybercrimes, now the governments of the states and other organizations are becoming cautious and considering the cyber security issues as the threat and working to deal with these as well. There is a common cyber security threat of stealing data from the organisations such as data breaches. Most organisations fall prey to the attack of classified data hacking by outsiders. The major challenge to the cases of data breaches is the rapid transfer of data from an organisation to an organisation. The cross-border nature of the incident of data breaches can make both the investigation and the separation of breach management options into an overwhelming and irresistible approach.

In recent years, The Asia–Pacific area has witnessed a flurry of new digital security regulations enacted in recent years, with countries establishing agencies or regulators to monitor and manage cyber security issues and publishing regular guidelines and circulars. In 2015, countries in East Asia such as Indonesia and Singapore established cyber agencies, and Japan passed the Cyber Security Basic Act. All of a sudden, Asia Pacific nations have started to formulate laws and/or guidelines as a

part of their attempt to secure their cyberspaces. If we look back to the other parts of the world, we already know that the Australian Securities and Investments Commission has issued cyber resilience. Meanwhile, in countries like the United States, its Justice Department issued a guideline titled "Best Practices for Victim Response and Reporting of Cyber Incidents" in April 2015. Many other countries are also adding cyber security guidelines to their existing frameworks.

Despite intensive measures by the government in the Asia–Pacific region, there is no evidence of taking a concerted approach in formulating cyber security regulations or possible legal action against the data breaches in the region. In addition to cyber security laws, the issue of data breaches can be incorporated into various existing laws and regulations. It may be incorporated with data protection laws and labour laws. It can also be integrated into the rules and obligations like equity rules, corporate governance and fiduciary duties. In some cases, the laws or legal frameworks of a state come into force when any data goes beyond the jurisdiction of any authority. Similarly, it is important to have local knowledge of the responsibilities of states and how regulators or courts are responding to data breaches. Besides, it is also important to know the best ways of legal remedies to the cyber menace. After acquiring the knowledge, the victim or who might fall prey to a cyber-attack can check whether there are any data cracks in his system. It may then be possible to separate the obligations to create a plan to limit further leaks of data. They can control and realize the impact or loss of data breaches, where they will find accessible and legal solutions to recover data or damage from data breaches. Many government websites rely on international servers and providers, putting them in a vulnerable position and putting them at risk of being hacked by system insiders [1]. The fourth category may pose the greatest threat to a country's security. This is a state-sponsored cyber-attack intended at undermining a national security framework, such as essential infrastructure or key national economic components, in order to gain strategic advantages over that country [17]. The example of China might be used as an example. Some of the world's most powerful countries, including the United States, the United Kingdom, France, Germany, and India, have long viewed China as a possible threat to cyber security and have accused it of espionage to obtain strategic advantages. It has been proven that in 2007, China launched a series of network-based cyberattacks against the countries listed above. Furthermore, these countries have stronger goals to improve their military's potential to participate in information or cyber warfare if it becomes required in near future.

3 Cyber Violence Against Women in Bangladesh Coontext

Women always fall victim to violence and harassment, including stalking, cyber-bullying and other forms of nuisance in Bangladesh. Apart from the harassment, pornography-related issues are also taking place here due to the easy accessibility of the internet and its ancillary equipment. After all, the cyber violence against women

goes unabated in the country's periphery with the same pace of the extension of Information and Communication Technology (ICT) and flourishing use of the internet due to lack of legal protection. Such violation of human rights stretches from stalking to cyberbullying and trolling which sometimes ended through reprisal pornography. Usually, the women are targeted from unidentified and counterfeit sources on the internet. They are given various types of ignominious messages frequently with obscene gestures. The women threatened them with nude pictures by placing the targeted women's faces in a photo with another nude photograph. The criminals also send spam, and sex-act tapes to make them frightened or lure them to do whatever the criminals want. Such types of unlawful things are now a new dimension of social media here. Especially with easy access to the smartphone, the active users of the internet have increased dramatically in Bangladesh. Of 90.5 million mobile phone users as of August 2018, 80.47 million are connected to mobile Internet [5]. Thanks to the additional use of mobile phone internet, the number of Facebook users has surged in the country. About 86 percent of 29 million registered Facebook users use social media sites through mobile phones. However, the number of females who have access to the internet through mobile phone sets is only 1 per cent. However, young women fall victim to sexual violence comparatively than the ageing women in Bangladesh. As a result of the lack of a legal framework and organizational protection, a sizeable 73% of women Internet users in Bangladesh lodge formal complaints regarding cyberspace pestering, abuse, and violence emanating from Cybercrime [18]. Amid huge frequent incidents of cybercrime in Bangladesh, the government has been forced to open a help desk to deal with the crimes. As of December 2017, the government's "Cyber-Help Desk," which is part of the Information and Communication Technology Division, has received over 17,000 complaints, with women accounting for 70% of the complainants. The risk of exposure to pornographic content is much higher among young people. Whether it is intentional or unintentional. In most cases, they are victimized by pornographic photos in the country. Around 78 percent of occurrences of doctored images with pornographic content in the digital world involve women. It should be emphasized that roughly 77 percent of Bangladeshi youths watch pornography on a regular basis.

According to a report by the Bangladesh National Association of Women Lawyers in June 2019, it is stated that harassment prevails in society with a concerning instance and several young women drop out of classes or jobs due to trauma and stigma as there are inadequate preventive measures and legislation. Court orders mandating the formation of complaint committees and the installation of complaint boxes in educational institutions and workplaces have been rarely executed [16]. In Bangladesh, it is very common for social media accounts to be hacked with vicious intentions. The criminals usually post doctored obscene pictures relating to the victims and then send provocative messages to the women to victimize them. Most of such incidents happen by smearing the victim, taking revenge, forcing them to establish sexual contact, threatening them with extortion or physically tormenting the victims. Conducting a study on the lawsuits and media reports, it is found that most of the cyber violence against women are happened in Bangladesh to establish physical contact with the victims. Usually, the offenders capture or collect photos or videos of

any intimate moments, and materialized their further evil wishes—it may be sexual contact, extortion or any other unlawful demand—by threatening the victim further with the weapon. Besides, the criminals captured the videos of rape scenes so that they can use these recordings to silence the victims. Most of the time, those video clips are released by the criminals despite the request of the victims not to publish them. There could be nothing more than this way of humiliating, traumatizing and stigmatizing a woman in society in such a way. There are numerous reports of committing suicide of women as they feel utterly helpless after experiencing such nightmares. Another common trend is found that vindictive ex-husbands and former lovers release intimate videos or pictures on social media platforms tenaciously. After all, young women are most vulnerable to falling into the traps of cybercriminals.

3.1 Effects of Cyber Violence

The impact of cyber violence on women in the conservative society in a country like Bangladesh is far-reaching, horrible and deep rooted. Here, victims' families are also victimised and traumatized along with the victims. There are numerous incidents in the country where the reprisal of both the victims and their families comes as a double blow. Thanks to the ignorance of the majority of people in the least developed countries like Bangladesh, most people strongly believe whatever content they see on social media platforms. If any photographed picture of a woman released on social media or any online platform matches any mixed up with vulgar gossip, most users do not think of verifying the picture and indiscriminately share the fake content, making it viral on the online platform. This proclivity for spreading sex-related rumors exacerbates the victims' pain, as well as the sorrow of the victims' family members, who endure social marginalization, shame, and public hatred [10]. As a result, if any doctored nude photograph is published on the social media sites defaming any women, they believe it blindly. Then the woman was slandered. In some cases, the victim's family is kept in confinement. In many other cases, the victim was evicted from his home or village. So cyber violence creates a catastrophic situation in the personal life of the victim. As a result, they suffer from severe depression, guilt, and paranoia. Their careers, education and social life are endangered. As a result, many of them became drug addicts. Some people decide to end their lives because they can't stand the stress. Very few of the victims were able to recover from the trauma. From 2010 to 2014, Bangladesh National Women Lawyers Association attempted to commit suicide among 65 female victims of such violence. Of these, only 11 women victims of cyber violence have attempted suicide. The number of such cases was only 8 in 2008, the data reveals an upward trend. However, the official statistics are paltry in comparison to the actual number of such incidents, with the number of unreported cases far outweighing the reported ones [4].

4 Challenges to Bangladesh and Bangladesh Government

Bangladesh is one of the highest cybercrime vulnerable countries in the world as most of the software used here is pirated. Besides, the infrastructural system is also poor. In such a situation, this is a big challenge to protect the country's cyberspace. Around 90% of software is pirated in Bangladesh [3]. Usually, when pirated software is used, criminals can penetrate easily due to the system loopholes. But, in Bangladesh, no one bothers about whether they are using the software that is pirated. This is one of the reasons for the vulnerability of the country's cyber security domain. Though this issue is ignored, many users pay the price when they have no other ways to fall victim to cybercriminals and its consequences and impact cannot be ignored. Besides, there are some other serious challenges for those criminals who target the people here most and carry out any cybercrimes staying out of reach and punishment. There were 90.5 million active internet users in Bangladesh as of August 2018, data from Bangladesh Telecommunication Regulatory Commission (BTRC) showed. Not at all, 1.8 million new connections were added to the network in one month. Of them, 84.7 million users use mobile Internet. About 5.73 million of them have fixed broadband Internet connections, while the rest use WiMAX connections. In April 2017, the total number of active Internet connections surpassed 70 million, followed by 60 million in August 2016, 50 million in August 2015, and 40 million in September 2014. (*The Daily Star*, 21 September 2018). Bangladesh's banking sector is under considerable cyber threat as a result of the country's rapid expansion in Internet usage. So a strong built-in cyber security is needed in such situations. At the same time, there is a need for experts to protect knowledge and data related to cybercrime.

First and foremost, we must comprehend these difficulties. We must be aware of the extent of daily cybercrime. There are four different sorts of cybercrimes that commonly occur in the country. Hacking, illegal entry, spying, data infiltration, e-mail spoofing, spamming, fraud and forgery, slander, drug trafficking, and virus transmission are examples of crimes against humanity. Second, property-related cybercrime is a subset of cybercrime. Credit card fraud, intellectual property infringement, and internet time theft are just a few examples. Organized crime is the third category of crime. Unauthorized control/downloads from network resources and websites, posting obscene/pornographic content on the web, virus attacks, e-mail bombings, logic bombings, Trojan horses, data dodging, download blocking, theft of valuables, government terrorism against organizations, and network infrastructure vandalism are just a few examples. The fourth and last type of f cyber-crimes is the attack on Bangladesh's society or social values, with such crimes including forgery, online gambling, prostitution, pornography (especially child pornography), financial crimes, the pollution of youth by indecent exposure, and web jacking, etc. [11]. Pornography has become a matter of major concern in Bangladesh. Pornography is strongly prohibited in the country in terms of the country's social culture and moral values. One of the reasons for this is the rapid expansion of digital communication technology. Because, as a result, it is now possible to communicate instantly with anyone from anywhere in the world to anywhere else. As such, it has become easier

to share and exchange the cultural values of an individual or a country. Therefore, due to the free spread of culture, many harmful elements of the culture of another country can easily penetrate their own culture. Which cannot be adapted in any way to one's own culture. Extremely unpleasant elements of perverted culture like pornography are in no way acceptable in the culture of Bangladesh.

Bangladesh's law enforcement agencies regularly receive numerous allegations of sexual harassment. These sexual harassments include secret nude video footage or posting obscene pictures demanding large sums of money. Or publishing these videos and nude photos for defamation. This type of crime is also committed as a result of previous hostility, failure to fulfil any evil desire or enmity with another member of the family. Most of these victims are teenagers. However, women and children are not the targets of criminals. If a crime is committed outside the country, it is considered a Trans boundary crime. Then it is considered a crime in both the countries where the crime was committed and the country in which it was located. However, it is not an easy task to bring cybercrimes like pornography under the law, especially in the context of Bangladesh. Because pornography is not considered a crime in many countries. In many countries, such as the United States, it is not considered a crime. Therefore, these Trans boundary crimes have to face various problems. However, child pornography is an international crime. Such a crime is considered a crime in any country. International assistance is available to deal with these crimes. Such a case is fully described below.

Several years ago in Bangladesh, Tipu Kibria, a well-known children's writer, was arrested by the police with evidence of child pornography. She used to come to her house and lab with male street children and make pornographic videos. He assaulted about 400–500 street children before his arrest. Kibria used to do all these things with the help of his two assistants. Police later found the names of 13 foreign shoppers who regularly paid Kibria to supply child pornography through online banking. Apart from Tipu Kibria, Bangladesh Police believe there may be other makers of this form of pornography. As a result, it is apparent that pornography is a big threat to Bangladesh's cyber security [1]. Cyber security threats and online banking in Bangladesh are now a matter of great concern for all types of financial transactions. Due to the potential for illegal online transactions, international criminal gangs carry out various criminal activities in Bangladesh, including drug smuggling, trafficking and terrorism, which represent a challenge to the country's cyber security. Bangladesh's banking sector is under severe cyber threat due to a lack of proper cyber security measures. Hackers stole $101 million from Bangladesh's central bank using the Swift payment network for counterfeit orders from the Federal Reserve Bank of New York. Which is one of the biggest cybercrimes in the history of cybercrime. The main reason behind the scandal of such a big economy is the weakness of the cyber security system. Lack of proper defence business. If Bangladesh still fails to ensure cyber security, then the country's banking sector may face more such cyber thefts in the coming days. A vast amount of personal client details, such as bank account names, bank account numbers, cell phones, e-mail IDs, and so on, are often put in danger when credit cards and electronic payment methods are used extensively [3].

Law enforcement agencies in Bangladesh often receive complaints about direct or indirect cyber threats to financial transactions through online banking. On February 12, 2016, evidence of 21 suspicious card transactions was found from Eastern Bank, a private bank in Bangladesh. A fraudster browsed with a fake EBL card from an ATM booth at United Commercial Bank Limited. On February 25, the Dhaka Metropolitan Police said that while investigating the ATM card scam, they found the involvement of various hotels and travel agencies. Some bank officials are also involved in this. Police also arrested three people, including a German national named Piotr, on charges of ATM fraud. Police have found evidence of the involvement of some employees of Citibank, a local private bank, in the scam. It was later revealed that Piotr was wanted in at least three countries for fraud (*The Daily Star*, 26 February 2016). In Bangladesh, foreigners are involved in financial scams, including money laundering from ATMs. They are targeting Bangladesh due to the inadequate security of the digital financial transaction system in the country. A number of recent financial scandals have alarmed banks and consumers. In February 2016, lawyers for Bangladesh Bank and three other commercial banks analyzed video footage of four ATM booths and found that at least Tk 2.5 million had been looted. The spokesperson for the central bank said that the principal perpetrators were at least two foreign nationals. Similar concerns affect other private banks, such as Eastern Bank Limited, United Commercial Bank Limited and Citibank, all of which have been victims of ATM fraud (*The Daily Star*, February 16, 2016). Following a spate of illegal transactions, all banks, including both public and private commercial banks in Bangladesh, are currently tightening security. But there are questions about whether those security measures are appropriate. Why is there a lack of technology to ensure proper security? Besides, those in charge of security lack knowledge. As a result, the banking sector in Bangladesh is still struggling to ensure cyber security. Also, many people in Bangladesh are victims of fishing or fraudulent attempts. They are enticed by emails or attractive advertisements to steal all their money after taking confidential data such as usernames, passwords and credit card details. Victims often lose $100–500 in each case and are often hesitant to report the crime to the authorities, making the situation in Bangladesh even more difficult to deal with [1]. Hacking, or unauthorized access to a computer system without the owner's or user's consent, is also a cyber-security risk in Bangladesh [11]. Before committing any financial crime, hackers typically closely monitor the financial activities of both government and non-government entities, looking for holes in the transaction system. Bangladesh is in a more difficult position to combat cyber-piracy due to a weak cyber infrastructure network and reliance on overseas server system providers, among other things, due to a lack of competent cyber security know-how [1]. In addition to the concern of digital financial fraud in Bangladesh, another concern is the theft of information or data. In 2014, a very sensitive verdict (partial) of the Bangladesh War Crime Trial Tribunal was leaked. The data of the tribunal was leaked through Skype's voice recording and caused a major backlash against the Bangladesh government and exposed the vulnerability of cyber security in Bangladesh [1]. Meanwhile, the lack of cyber security on social media platforms has become a serious threat to the citizens and the government in Bangladesh. Unpleasant incidents are constantly happening, especially on Facebook, Twitter and LinkedIn

due to a lack of proper security measures. The incidents like social media account hacking were frequent until February 2019. The hackers mostly hacked the social media accounts of celebrities, celebrities and women and demanded large sums of money in return. Without money, they would ruin the social image of the victims. At one stage, the law enforcement agencies of Bangladesh, especially the police, were forced to form a monitoring team to strengthen their monitoring. Besides, Bangladesh Telecommunication Regulatory Commission has also formed a separate monitoring team to control the crime.

5 Existing Acts Related to Cyber Security and Their Limitations

Despite repeated incidents of cybercrimes, so far there is no headache or concern about the existing cyber security measures or risks in the country. Despite considerable concerns, the country has not been able to properly and timely address the risks. Due to a lack of understanding among the various stakeholders concerned, the concerned authorities are also unwilling to take full action to deal with any approaching risk. To combat cyber-crime, the Bangladesh government has enacted the Information and Communication Technology (ICT) Act and the Digital Security Act. There is a lot of criticism among the rights activists and intellectuals of the country about some articles about those acts which are considered weapons of throttling the media and public opinion. Sadly, these laws are being used to punish critics of the government or government party political parties. It is being used as a tool to curb the freedom of speech of ordinary people. With these laws, the government and law enforcement agencies have cracked down on the media and social media in the country. In the face of much protest and criticism, on 8 October 2006, the Bangladesh government passed the ICT Act in the parliament. In the face of strong criticism, seven years later, the government amended the law on October 6, 2013, tactfully keeping the controversial provisions of the law intact. Victims in Bangladesh can at least use this ICT Act as a starting point; however, strong cooperation is required to progress from regional law enforcement agencies with expertise in cyber security, such as the CID (Criminal Investigation Department), to international law enforcement agencies, such as Interpol [1]. Section 57 of the Information and Communication Technology Act provides ample scope for the misuse of this Act. Human rights, lawyers, civil society representatives and media critics have all called for the repeal of the act. Before the amendment of the act, the convict was liable to imprisonment for a term not exceeding 10 years and a fine of Tk 10 million if convicted. Law enforcement agencies had to seek the permission of the appropriate authorities to file a case before arresting a person under this Act. Following the 2013 amendment, the maximum prison term has been set at 14 years. Moreover, law enforcement agencies are given unilateral power. As a result of the amendment, law enforcement agencies can now detain anyone without a warrant. Despite strong criticism and protests from

human rights lawyers, civil society representatives and the media, the government has remained steadfast in its stance on the issue. Section 57(1) states, "If any person deliberately publishes any material which is false and obscene or transmits or causes it to be published or transmitted on the web, or in any other electronic form, and if anyone sees, hears or reads it having regard to all relevant circumstances and its effect is such as to influence the reader to become dishonest or corrupt, or causes a deterioration or creates the possibility to deteriorate law and order or prejudice the image of the state of a person or causes hurt or could offend religious belief or instigate against any person or organization, then this activity will be regarded as an offence". Despite reforms that made a few major changes, the core 2006 Act remains unchanged, with all of its flaws and needlessly punitive penalties [2].

The ICT Act (amended) has now been used as the tool of the Bangladesh government to curb fundamental human rights. Freedom of opinion and expression is now at stake as the act has a range of ambiguous clauses [9]. This act will encourage instigating cybercrimes instead of containing cyber-criminal activities. According to the ICJ, The original ICT Act's Section 57 is "incompatible with Bangladesh's responsibilities under Article 19 of the ICCPR: the charges imposed are unclear and disproportionate, and the limitations on freedom of speech and opinion go beyond what is permissible under Article 19 (3) of the ICCPR," according to the ICJ (ICJ, 2013). "Section 57 is not explicit and encompasses a broad range of offenses," J. Barua explained, "and there is minimal likelihood of winning an acquittal from any accusation" [2]. After studying the ICT Act 2006 and its revisions, it is clear that new legislation is needed to combat cyberspace-related crimes, as the current Act is confusing and has to be built permanently as a modernist legal structure rather than being based on an ad hoc approach (*The Daily Star*, 2013).

Human rights activists and journalists have been critical of Section 57 right from the very beginning of the enactment of this law. But the criticism sparked a protest after a senior journalist named Probir Sikdar was arrested in 2015 under Section 57 of the ICT Act. In addition, in the four months leading up to July 2017, at least 21 journalists were sued under Section 57 of the Information and Communication Technology Act, despite mounting calls to repeal the provision, which is widely prone to abuse (*The Daily Star*, 7 July 2017).

Amid widespread criticism, Bangladesh's Law Minister Anisul Huq on May 2, 2017, said "Section 57 would be withdrawn and that a new "Information Technology Act that is in the pipeline" will be implemented." But later on September 19, 2018, Bangladesh's Parliament passed the Digital Security Act, incorporating another tough clause empowering the law enforcement agencies to search or arrest anyone without a warrant creating further outcry among the rights activists and journalists. They have been expressing concern saying that the act goes against the constitutional rights of the country's people and it will curb freedom of expression and gag the media. Section 43 of the Digital Security Act states that when a police officer believes that a crime has been committed or is taking place in a specific place where there is a risk of crime being committed if the evidence is lost, the officer may search the location or arrest any person. The Editors' Council, (Sampadak Parishad), the council of the editor of news media in Bangladesh, stated on September 16, 2020, expressed

surprise, frustration, and shock over some sections of the Digital Security Act. In their statement, the editors stated that Sections 8, 21, 25, 28, 29, 31, 32, and 43 of the Act pose serious threats to freedom of expression and media operation. Section 3 of the Digital Security Act incorporates a clause of the Access to Information Act 2009 which will be extended to information-related matters. According to the section, if a person uses a computer, digital device, computer network, wireless network, or any other electronic medium to commit any crime or assist others in committing crimes under the Official Secrets Act, 1923, as provided for in Section 32 of the law, he or she may face a maximum of 14 years in prison or a fine of Tk 2.5 million or both. A definition of the "Spirit of the Liberation War" has also been included in Section 21, which states, "The high ideals of nationalism, socialism, democracy, and secularism, which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in the national liberation struggle." However, under Section 29 of the law, a person can be sentenced to three years in jail or snapped a fine of Tk 500,000, or both if he or she is found guilty under Section 499 of the Penal Code for his crime online. Section 31 states If a person published or broadcast something on a website or in electronic form that could spread hate and build enmity between different groups and communities, or that could cause a deterioration in law and order, he or she could face seven years in prison or a fine of Tk 500,000, or both penalties (*The Daily Star*, 20 September 2018).

6 Policy Opinions

In addition to reducing the rate of cyber-crime, several alternative remedial policies can be implemented to ensure cyber security in Bangladesh. The government of Bangladesh may consider the following alternative policies.

6.1 Reform of the Legal Structure

We fully support the recommendations of the ICJ regarding the ICT Act 2013 of the Government of Bangladesh and its amended law. The ICJ called upon the Parliament of Bangladesh to implement these recommendations. In their recommendations, ICJ said, 'Either repeal the Information and Communication Technology Act (2006) as amended in 2013, or amend the ICT Act to bring it in line with international law and standards, including Bangladesh's legal obligations under ICCPR. The ICJ recommended that the Bangladesh government (1) amend Section 57 of the ICT Act to ensure that any planned restrictions on freedom of expression and opinion are in accordance with international law and standards; (2) amend Section 57 of the ICT Act to ensure that forbidden speech is clearly defined; and (3) amend the ICT Act to ensure that any restriction on freedom of speech and information, including any penalty imposed, is necessary for a valid purpose and proportionate to that purpose [9]. The

ICJ also proposed several policies—(i) Take action to ensure that the provisions of the ICT Act are not used to infringe the right to freedom of speech, including restricting the legitimate exercise of public opinion on matters which could include criticism of the Government; (ii) drop charges against bloggers for the legitimate exercise of their freedom of expression; (iii) guide government agencies to refrain from unfairly limiting the freedom of speech in politically-motivated cases and not to pursue penalties that are disproportionate to the severity of the alleged offence [9].

6.2 Maintaining Rules of Cyber Security

Menken Tikk, the legal counsel at the NATO Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, wrote an article on 'Ten Rules of Cyber Security in 2011. In his article, Tikk came up with a framework to ensure cyber security principles considering the security concerns for personal and state levels. In many cases, the proposals made by Tikk are acceptable. For ensuring cyber security, Tikk proposed 'the territorial rule' where he stated, "information infrastructure located within a state's territory is subject to that state's territorial sovereignty" [15]. In his 'the law of duty ', Tikk suggested that a country must play a responsible role in ensuring cyber security in its territory. He also proposed an 'early warning statute', where he stated, "There is an obligation to notify potential victims about known and upcoming cyber-attacks" [15]. The rules that Tikk has proposed regarding cyber security can be implemented by any country in the world. We can also implement Tikk's proposal for Bangladesh to fight against cyber threats from Bangladesh.

Secondly, any state can adopt its 'data protection rule' to protect the crucial data of a state. Tikk also stated, "Information infrastructure monitoring data are perceived as personal unless provided for otherwise." We can mention another proposed rule of Tikk named "the duty to care rule". In his rule, he suggests that everyone takes a minimum level of responsibility to secure all kinds of information infrastructure [15]. In the light of Tikk's rules, we can propose that the Government of Bangladesh will formulate and implement a policy framework using its resources and expertise to safeguard the cyber system and national interests. The country's cyber experts need to be trained to become more efficient. Besides, the country needs to create its own "server framework and system" using its resources and labour, which will play a role in ensuring cyber security nets. For this, we have to recruit trained manpower. It will take a long time but it will be a sustainable cyber security system. This will reduce the dependence on foreign experts.

Thirdly, we also support 'the cooperation rule' of Tikk. Here he mentioned, "… a cyber-attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state" [15]. Fighting against any kind of cyber security risk requires strong global participation. Because, in addition to local threats, in most cases, cyber threats come from the international arena. A criminal can harm a person or an organization from one country to another, or commit a crime in one country and flee to another. Therefore, the suppression of such a crime

requires global support and participation if necessary. The Bangladesh government and the Bangladesh Police are liaising with international law enforcement agencies such as Interpol. In addition to strengthening that communication, we need to work for cooperation from other law enforcement agencies and tech giants around the world, such as Microsoft, Google, Facebook, Yahoo and others. Besides, we can also adopt Tikk's other two rules—'self-defence and access to information. He Tikk said, "Everyone has the right to self-defence" and that "the public has a right to be informed about threats to their life, security, and well-being" [15]. Finally, for ensuring cyber security at both the individual and national levels, we are strongly recommending the Government of Bangladesh take all precautionary and necessary measures.

6.3 Individual Awareness

In the current era of globalization, change and changed reality are undeniable. If anyone can't adapt to that change and can't cope with any of the shocks that come with that change, survival will be extremely difficult. In this ever-changing cyber world, to protect personal data alongside national information, we should have awareness at the individual level as well as the government needs to create secure cyberspace. Professionals must achieve a minimal degree of proficiency in handling cyber technologies and establish knowledge of cybersecurity threats, regardless of their hierarchy or organizational structure. Bangladesh can only be saved from sliding into a deep pit of cybersecurity risks if it receives sufficient education and awareness (Alam, Md. Shah, personal communication, 27 July 2014).

The basic precautionary measures need to follow while using the internet:

- Keeping personal details in restricted mode if necessary;
- Keeping privacy settings on;
- Using secure browsing;
- Using sure internet connection;
- Using strong passwords;
- For online transactions, browsing from protected sites;
- Being careful about any type of post;
- Keeping antivirus software updated.

If you somehow realize that you are a victim of cybercrime, then you should go to the local police station without any negligence. In addition to seeking the cooperation of the police, it is necessary to inform the matter to the relevant organization or medium. If it is a financial scam, then you have to contact the concerned financial institution. If any occurrence happens on any social media platform, you have to communicate with the respective platform. Depending on the situation, higher levels such as the FBI and the Federal Trade Commission may be contacted. If we are active from the beginning, it will be possible to prevent the recurrence of such crimes.

7 Conclusion

In conclusion, the issue of cybercrime has become a potential threat to the national security of any country, not just Bangladesh. However, in the context of globalization, the issue of cybercrime is even more worrying for a country like Bangladesh, especially where there is no secure cyber system. Due to the lack of advanced cyber security tools in Bangladesh and the ignorance of the people about the use of technology, use of unsafe technology, lack of necessary laws and indifference of the government, Bangladesh and the people of this country are a serious cyber security risk, which may lead to a devastating situation in the state. Another thing is that there is no publicity about cyber security in the country. There is no campaign or initiative to inform the people about the law of Bangladesh, cyberspace and international cooperation, increase technical knowledge and skills and what to do about cyber security threats. So these issues need to be taken into consideration to combat the ever-looming cyber security threats. However, the rapid increase in cybercrimes in Bangladesh and around the world proves that the issue of cybercrime is undeniable. Someone may argue that the cyber threat is not a major threat to Bangladesh right now. But in the light of the present situation, it can be said that these arguments have no basis, only conjecture. Finally, it needs to be said that Bangladesh should take immediate and preventive measures to curb cybercrime right now. Hopefully, the recommendations given in this research paper will play a vital role in ensuring cyber security for the Government of Bangladesh and the people of the country.

References

1. Alam S (2019) Cyber Crime: a new challenge for law enforcers. City Univ J 2 (1):75–84. http://www.prp.org.bd/cybercrime_files/Cybercrime. Accessed 25 Apr 2020
2. Barua J (2019) Amendment information technology and communication act. The daily star. http://www.thedailystar.net/supplements/amended-information-technology-and-communication-act-4688. Accessed 25 May 2019
3. Bleyder K (2012) Cyber security: the emerging threat landscape. Bangladesh Institute of Peace and Security Studies, Dhaka
4. BNWLA (2014) Survey on psychological health of women. Bangladesh National Women Lawyers' Association, Dhaka
5. BTRC (2018) Internet subscribers. Bangladesh telecommunication regulatory commission. http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-april-2018. Accessed 12 May 2020
6. Editorial (2013) Draft ICT (Amendment) Ordinance-2013: a black law further Blackened. Daily Star. http://archive.thedailystar.net/beta2/news/draft-ict-amendment-ordinance-2013. Accessed 25 Dec 2019
7. Greenemeier L (2007) China's cyber attacks signal new battlefield is online. http://www.scientificamerican.com/article/chinas-cyber-attacks-sign. Accessed 12 Aug 2019
8. The Information & Communication Technology Act (2006) The Information & Communication Technology Act. http://www.prp.org.bd/downloads/ICTAct2006English.pdf. Accessed 11 July 2020

9. International Commission of Jurists: Briefing Paper on the Amendments to the Bangladesh Information Communication Technology Act (2013). http://icj.wpengine.netdna-cdn.com/wp-content/uploads/2013/11/ICT-Brief-Final-Draft-20-November-2013.pdf. Accessed 10 May 2020
10. Karaman S (2017) Women support each other in the face of harassment online, but policy reform is needed. The LSE women, peace and security blog. The London School of Economics and Political Science, London. http://blogs.lse.ac.uk/wps/2017/11/29/women-support-each-other-in-the-fa. Accessed 1 Mar 2020
11. Maruf AM, Islam MR, Ahamed B (2014) Emerging cyber threats in Bangladesh: in quest of effective legal remedies. North Univ J Law 1(2010):112–124. https://www.banglajol.info/index.php/NUJL/article/view/18529. Accessed 21 Aug 2020
12. Elahi SM (2014) Porn addicted teenagers of Bangladesh. Manusher Jonno Foundation, Dhaka
13. Perlroth N, Gellesaug D (2014) Russian hackers amass over a billion internet passwords. http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet. Accessed 28 Jan 2019
14. Singer PW, Freidman A (2014) Cyber security and cyber war: what everyone needs to know. Oxford University Press, Oxford
15. Tikk E (2011) Ten rules for cyber security-survival: global politics and strategy. Routledge, London
16. USSD (2017) Country report on human rights practices for 2016. US Department of State, Washington DC (2017). https://www.state.gov/j/drl/rls/hrrpt/2016humanrights/report/index.htm?ye. Accessed 2 Aug 2020
17. Williams B (2014) Cyberspace: what is it, where is it and who cares? http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/. Accessed 15 July 2020
18. Zaman S, Gansheimer L, Rolim SB, Mridha T (2017) Legal action on cyber violence against women. Bangladesh Legal Aid Services Trust (BLAST), Dhaka