CIFILE Journal of International Law (CJIL), Vol. 5, No.9, 39-48 (2024)

Homepage: https://www.cifilejournal.com

Print ISSN: 2563-6820
Online ISSN: 2563-3341

A Critical Analysis of the Escalating Cybercrime and its Impact in Bangladesh

Md. Sohel Rana

Brac University, Dhaka, Bangladesh

(Corresponding Author) tanveersohel183@gmail.com

https://doi.org/10.30489/cifj.2023.407899.1075

ARTICLE INFO

Article history:
Receive Date: 19 July 2023
Revise Date: 14 December 2023
Accept Date: 28 December 2023

Keywords:
Hacking, Malware, Identity theft, Data, breach, Online Fraud

ABSTRACT

Cybercrime is a growing concern in Bangladesh, and this paper will critically analyze the nature and extent of cybercrime in Bangladesh and its impact on individuals, businesses, and the economy as a whole. The research will begin by exploring the various types of cybercrime prevalent in Bangladesh and the methods cybercriminals use to carry out these crimes. It will then examine the reasons behind the increase in cybercrime in Bangladesh, including factors such as inadequate cyber-security measures, low awareness among the public, and the widespread use of digital technology. Moreover, the research question for this paper is: What are the main causes of the growing cybercrime problem in Bangladesh, and what can be done to mitigate its impact? Finally, this paper also discusses the challenges faced by law enforcement agencies in tackling cybercrime and the measures that can be taken to address this issue.

Introduction

Wars in the near future will be fought over information rather than oil or borders. Whoever controls the most information will have the most influence in the not-too-distant future. That is why it is essential to have a conversation about crimes committed digitally. For instance, Russia is now a more powerful country because they are creating a virtual fight that is more capable of Hacking. These days, big-shot countries such as the United States and others are scared because of Russian hackers. This is because Russia is making an army that is more capable of Hacking. Russia is the only nation that significantly increased its spending in this hacking industry [1]. In February of 2016,

[1] Kundu A, ' Cybercrime trend in Bangladesh, an analysis and ways out to combat the threat' [2018] Electronic Journal https://www.researchgate.net/publication/324468211_Cyber_crime_trend_in_Bangladesh_an_analysis_and_ways_out_to_combat_the_threat Accessed 2 January, 2023

Bangladesh Bank, which acts as the Central Bank of Bangladesh, was the target of a cyber-robber on a scale that had never been seen before. Unidentified hackers made an effort to steal a staggering $951 million from the bank's reserves. They just took advantage of one of our bank holidays and utilized certain spam mail techniques to break into our system, both of which our bank employees overlooked in the first instance. There was some success in getting the money back, but it was not possible to get the full sum. The introduction of Information Communication and Technology has made communication and commercial transactions easier. Bangladesh is also entering the digital world, and the country is now labelled 'Digital Bangladesh' due to the prevalence of social networking sites in Bangladesh, which has a disproportionately high rate of cybercrime.[2] To be more precise, the majority of cybercrimes take place on Facebook. Facebook is by far the most popular and widely used social networking site in Bangladesh, with over 71 percent of the country's population having an account. When it comes to online privacy and the flow of information, few people in Bangladesh seem to care. This is a major factor contributing to the exponential growth of cybercrime in Bangladesh. A large portion of the population doesn't appear to care much about cybercrime and related legislation.

1. Historical Background

Since technology advances, humans are becoming increasingly dependent on automation. It has a significant impact on every facet of society and life. The history of automation began with Babbage's invention of the computer, and a new era was opened with the development of networks, particularly the Internet and the World Wide Web (WWW). In 1997, Internet use advanced. By 2005, 180 ISPs were operating after the government liberalized national rules to support and accelerate sector growth. In 2006, Bangladesh got connected with Submarine Cable, which afforded bigger bandwidth and lower costs than ever before. [3] Sheikh Hasina, the then-leader of the opposition in parliament, received a death threat in an email sent to the Bangla daily "Prothom Alo" on August 23, 2004. Two days later, the then-prime minister Khaleda Zia, her eldest son, and certain members of parliament all received death threats in another email. These two instances of cybercrime were the first ones.

The Rapid Action Battalion's (RAB) website was breached in 2008. Immediately following the Prime Minister's inauguration on January 10, 2010, 19 of the 64 district websites were compromised on March 21. Hacking Bangladesh's Central Bank in a recent assault on government territory resulted in the theft of national reserves. In Bangladesh, cybercrimes basically began at that point, and they now often lead to cyber fraud.[4] Bangladesh has a disproportionately high percentage of cybercrime in

[2] Kabir SE, 'Why Are Our Digital Laws so Troublesome?' (The Daily Star, 20 December 2022) <https://www.thedailystar.net/opinion/views/news/why-are-our-digital-laws-so-troublesome-3200866> accessed 1 November 2023

[3] Borhanuddin, A., 2016. 'Cyber Crime and Bangaldesh Perspective' Journal of Dhaka University, Department of Law, https://www.academia.edu/4488760/Cyber_Crime_and_Bangladesh_Perspective

[4] Alam, A 'A New Challenge For Law Enforcers', (2004) American Journal of Public Health, 94(6 951-957. https://www.justice.gov/d9/202306/wellness_challenges_for_law_enforcement_personnel_2; Accessed 1 November 2023

comparison to other countries because of the proliferation of social networking sites in the country. When Bangladesh first connected to an underwater cable in 2006 and its citizens started using social networking sites like Facebook and Yahoo Messenger, the country had not yet experienced any instances of cybercrime. On the other hand, when cell phones and internet access became more generally available, the number of crimes related to social networking sites began to grow and has continued to rise ever since.[5] Facebook, to be more specific, is the location where the majority of online crimes are committed. In Bangladesh, approximately 71 percent of the population has a Facebook account, making it by far the most popular and widely used social networking site in the country.

According to a study that was published in The Financial Express on January 10, 2008, Bangladesh has become a safe haven for computer thieves due to the fact that there is no active cyber law and a lack of expertise to uncover cybercrime.[6] According to the findings of Net, a company based in the United Kingdom that conducts research and analysis on internet applications, Bangladesh is one of the top 10 servers for fraudulent websites that host bogus websites or send fake emails in an effort to steal personal information. Even though the Information and Communications Technology (ICT) Act of 2006 covers many of the legal components to prosecute cybercrime, it has not been adequately applied since its ratification, which means that criminals who engage in cybercrime can easily dodge consequences in Bangladesh.[7] There are five factors that have a direct and indirect effect on the occurrence of cybercrime.

Individual factors:

1- Age: The study of cyber criminology cases generally states that there is an inverse relationship between crime and age.

Societies whose age pyramid is narrower at the base (so-called old societies) have a lower computer crime rate.

2- Gender: research shows that there is a direct relationship between the gender of users and the rate of visiting porn sites. 82% men and 5% women

3- The level of technical skills and internal talents:

In the past, it was thought that hackers and cybercriminals were highly intelligent and knew at least a few programming languages and computer security, but today, most computer crimes are committed with minimal skills. One can consult with hackers and purchase automatic software.

4- Education: According to the statistics of a study among first to fourth-year students in Canada, 88% of the participants have been involved in computer criminal behaviour. It can be concluded that young people and students or educated people can be identified more as computer criminals.

5- Family background and job field: According to the surveys, computer criminals can be from any class and are not limited to unemployed and low-income people. Even some internal cyber attacks are carried out by people who have wide powers.

[5] Ahmed SM, Hossain MdM and Haque MdM, 'Usage of Facebook: Bangladesh Perspective' (SSRN, 26 October 2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2167116> Accessed 14 November 2023

[6] Chen S and others, 'Exploring the Global Geography of Cybercrime and Its Driving Forces' (Nature News, 23 February 2023) <https://www.nature.com/articles/s41599-023-01560-x> accessed 14 November 2023

[7] 'Five Factors Influencing the Cyber-security Threat Landscape' (Security Magazine RSS, 14 August 2019) <https://www.securitymagazine.com/articles/90718-five-factors-influencing-the-cybersecurity-threat-landscape> accessed 14 December 2023

6- Criminal background: A study on computer criminals showed that more than 80% of the criminals had no criminal record, and only 20% were convicted of crimes such as drug dealing, gambling and selling obscene CDs. However, the lack of criminal record is not a reason for low risk; the committed Act and the injuries are important.

Environmental factors:

The virtuality of cyberspace and the possibility of multiple and false identities and their non-disclosure help cybercriminals commit crimes without worrying about revealing their true identity.

With the emergence of e-government and centralized databases of personal data, all the information of a person, from the date of birth, etc., is accessible in cyberspace. In the cyber world, criminals see everything they want in one place: national security, public and private agents. So, with the collection of all matters and information in the cyber world, an ideal city has been created for computer criminals to have access to any type of criminal purpose in a single environment. Information technology has enabled criminal groups to communicate anonymously with other criminals around the world and identify their victims with just one click.

2. Laws of Bangladesh:

A person's right to free speech is universal. In order to protect people's credibility and standing, this privilege may be curtailed. There can be no constitutional limits placed by law on the right to freedom of expression.[8] It's possible that the restriction is justifiable in the name of maintaining a liberal democracy. One's right to free expression through speech, writing, and other media may be overridden in a civilized society if it is used to maliciously smear another person's good name through the dissemination of incorrect or false information.[9] The misuse of a right can lead to inappropriate and unwelcome behaviour, both of which are illegal under Bangladesh's Penal Code (Act No. V of) 1860 and the Information and Communication Technology Act (No. 39 of) 2006, respectively. This is because the Act of 2006 does not address the majority of cybercrimes or digital crimes.

For example, crimes conducted using mobile phones are not included in this category.

[10] The current globe, including Bangladesh, is witnessing the development and continuation of a variety of cybercrimes, and this trend is expected to continue. Intrusions into computer systems without authorization, such as Hacking or the introduction of viruses tampering with or publishing pornographic material in an electronic format, are violations of the law. Electronic documents are required to be retained under law. Frauds committed using electronic documents, violations of privacy rights such as stalking, infringements of copyright, trademark, or patent design, defamation committed via email, and the making of threats via email are a few instances of these types of offences. The Information and Communication Technology Act has a number of problems that need to be fixed. Sometimes, the law will step in and govern the social norms and regulations that pertain to information

[8] Information And Technology Act, 2006 https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf

[9] The Penal Code, 1860 http://bdlaws.minlaw.gov.bd/act-11/section-3203.html

[10] Ahamed A, (2010) 'Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies' The Northern University Journal of Law, https://www. 10.3329/nujl.v1i0.18529 ISSN 2218-2578 Accessed 10 January2023

technology. [11]Therefore, despite the fact that the Act addresses intellectual property rights, it does not address the rights and obligations of domain name proprietors. This is particularly problematic given that registering a domain name is the initial step in conducting business online. According to section 76 of the Information and Communications Technology Act of 2006, the offences cannot be recognized. In order for the victim to be eligible for compensation, a formal complaint must be filed with the relevant law enforcement authorities. This is the Act's most significant shortcoming. According to the provisions of the Act's section 68, a specialized court that would be referred to as the Cyber Tribunal would be established in each of Bangladesh's districts.[12] On the other hand, there is only one Tribunal that has been established so far in the Dhaka region. The resolution of cyber disputes is uncommon since laypeople are reliant on the expertise of technological experts, as well as on lawyers and judges who have received extensive legal training. The few cases that are really filed are the ones that are considered to be pending. In order to clear up this kind of backlog of cases, judges, attorneys, and other relevant specialists need to have adequate training and experience. The Bangladeshi police force has a unit called the "Anti-Cybercrime Department". This unit's objective is to safeguard citizens from online crimes such as libel, defamation, and the release of illegal photographs. Due to a lack of adequately trained staff, the Department has not yet been able to satisfy the needs of the general public. Because the plaintiff cannot be located, the case cannot get underway. [13] There is no way for the state to become a plaintiff and assume any responsibilities or liabilities. The Cyber Tribunal has not yet handed down any sentences or punishments to any of the criminals who have been brought before it. Criminals continue to commit crimes because they are under the impression that they will not be penalized for their actions.

2.1 Digital Security Act, 2018

The government and ruling party activists in Bangladesh's favored weapon to silence opponents and stifle their freedom of expression, especially online, is the Bangladesh Digital Security Act, 2018, which came into effect on October 1, 2018. [14]The evolution of a nation's politics can be seen in the letter of the legislation and in its aftereffects. With merely reasonable suspicion that a crime has been committed via social media, law enforcement officials are now authorized to make arrests, search locations, and confiscate equipment without a warrant under the provisions of this Act. The statute also allows the government to remove and prohibit internet content that criticizes its policies or exposes human rights abuses in the country. DSA instances have exceeded 1,500 in three years. Eight cyber-crimes tribunals oversee these cases. The right to freedom of expression is enshrined as a fundamental principle in the

[11] Khursid A, 'CYBERCRIME IN BANGLADESH:IMPLICATIONS AND RESPONSE STRATEGY'(2016) https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/download/82/74/149

[12] Information And Technology Act, 2006 http://dohatec-ca.com.bd/DohatecCA/ICTAct.jsp

[13] Mia A, (2021) 'CYBERCRIME AND ITS IMPACT IN BANGLADESH: A QUEST FOR NECESSARY LEGISLATION http://ijlljs.in/wp-content/uploads/2015/06/Cyber-Crime_Article_IJLLJS1.pdf

[14]Digital Security Act, 2018 https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf

Constitution of the People's Republic of Bangladesh, specifically Article 39. The DSA is extremely denunciative against the freedom of speech, which is a violation of article 39, and so section 57 is the one that has caused the most controversy. This DSA, on the other hand, has demonstrated a more repressive attitude regarding the right to freedom of expression. At least 1135 people were arrested in 732 instances filed under the Digital Security Act in 2020 across Bangladesh, as reported by Daily Prothom Alo. The majority of the cases were filed under the Act's 25th section and 29th section for allegedly damaging the reputation of the country or an individual. Before the passage of the Digital Security Act, a comparable allegation was filed under the questionable Section 57 of the Information and Communication Technology Act (ICT) (DSA) Of the fifty cases brought in 2020 against journalists, thirty-seven were successfully prosecuted (Digital Security Act: almost one thousand cases filed in two years, 2022).[15] The Data Protection Act (DPA) 2022 draft has similar problems with overly broad and imprecise terminology. As well as having several elements that are similar to DSA, the DPA has an overriding impact that eliminates the citizens' right to information, which goes against the citizens' right to read and be informed and the Right to Information (RTI) Act, 2009. However, the nature of "personal data" is not formally defined. Interestingly, whereas the English version of the DPA contains 66 sections, the Bangla version has 70. It's quite challenging to speculate on whether poor drafting, incompetence, or omission on the part of the relevant authorities is to blame.

3. Cases regarding cybercrimes in Bangladesh

Mushtaq Ahmed, who had been incarcerated since May 2020 for allegedly disseminating anti-government content via online media, passed away in a maximum-security facility in February 2021. A political cartoonist named Kabir Kishore and two others were arrested together with Mushtaq for allegedly violating Bangladesh's Digital Security Act by spreading false rumours about the government's response to the COVID-19 outbreak. [16] An investigative journalist named Shafiqul Islam Kajol was indicted on November 8, 2021, for publishing "objectionable" material regarding members of the ruling party. Even though he does not have a smartphone, farmer Abu Zaman is on the run after being accused of orchestrating the spread of misinformation on Facebook. Multiple juveniles across the country have been arrested for online scholastics and transported to juvenile detention facilities. Shahidul Alam was accused of violating Article 57 of the Information and Communications Technology Act and was apprehended on August 5, 2018. Online communication that harms the state's reputation was used as an accusation against Shahidul. From July 29 to August 8, 2018, a massive demonstration was held in Bangladesh in favour of better road security. The unlicensed bus driver who was in a hurry to pick up passengers and killed two secondary school kids in the capital city of Dhaka sparked the protest. Students demanded safer roads and stricter driving restrictions after the incident, and the news of the shows rapidly travelled across the

[15] Why Are Cybercrimes Going Unpunished?' (The Daily Star, 14 August 2022) <https://www.thedailystar.net/opinion/editorial/news/why-are-cybercrimes-going-unpunished-3094791> accessed 14 December 2023

[16] 'Bangladesh: Cartoonist Tortured, Writer Dies in Jail: Ahmed Kabir Kishore' (Amnesty International, 6 June 2021) <https://www.amnesty.org/en/documents/asa13/3800/2021/en/> accessed 14 December 2023

country. [17] He used Facebook Live to broadcast his coverage of a student rally for improved traffic safety and to deliver a speech. On the same day, he gave an interview to the Arabic news network Al Jazeera. On November 15, the High Court decided to release him on bond, and he was finally freed the following week on November 20. He had spent approximately 90 days in jail prior to this.

4.Impacts of Cyber Crime in Bangladesh

The growth of the telecommunications industry is essential to the advancement of science, information, and communication technology. This industry is not yet fully developed because there is not enough deregulation and not enough open competition. The effects of cybercrime are not particularly concerning for Bangladesh at this time due to the fact that online financial transactions are not yet fully functional. If the government does not invest in the technology and infrastructure necessary to prevent, detect, and prosecute computer crimes as soon as financial transactions can be conducted online, the number of computer crimes will skyrocket at an unprecedented rate. However, our government is still not aware of this fact. Some individuals make use of the Internet in order to spread deceptive and harmful information. Some of them engage in the trafficking of children and women via the Internet.[18] The distribution of pornographic material is yet another lethal and lucrative tool in the hands of cybercriminals. Nevertheless, the government of Bangladesh is not on high alert despite all of this.

Despite the fact that the Information and Communications Technology (ICT) Act of 2006 addresses a significant number of the legal considerations necessary to prosecute cybercrime, the law has not been successfully applied since it was ratified.[19] The absence of legal support as well as social and public knowledge regarding computer crimes, according to the opinion of the experts, is the primary factor that contributes to the ineffectiveness of the legislation. Analysts of cybercrime point out that despite the fact that pornography is not generally regarded as a criminal offence elsewhere in the world, it is one of the most common types of computer crime in Bangladesh. A variety of disruptive acts take place at these cafes under the guise of people just perusing the Internet, according to press sources.[20] There are separate rooms for couples to use for Internet browsing, and these cabins also include hidden cameras to record the couple's private interactions. After some time, these photographs were uploaded to the Internet for anybody to view. A person who is found guilty of posting vulgar and obscene content onto a website faces a fine of ten million Taka in addition to ten years in prison under the provisions of section 57 of the Information and Communication Technology Act of

[17] Ahmed Q, 'Why Did Bangladesh Arrest Shahidul Alam?' (Al Jazeera, 9 August 2018) <https://www.aljazeera.com/opinions/2018/8/9/why-did-bangladesh-arrest-shahidul-alam> accessed 14 December 2023

[18] Hosssain, D (2021),Bangladesh Cyber Crime Investigation and Judicial System https://www.academia.edu/4225890/Cyber_Law_Bangladesh_Perspective

[19] Department K-E-KBL and others, 'Cyber Legislation and Cyber-Related Legal Issues in Bangladesh: : Inadequacies and Challenges: International Journal of Electronic Security and Digital Forensics: Vol 13, No 2' (International Journal of Electronic Security and Digital Forensics, 1 January 1970) <https://dl.acm.org/doi/10.1504/ijesdf.2021.113379> accessed 14 December 2023

[20] Khadam A (Insight to cybercrime) <https://www.semanticscholar.org/paper/Insight-to-Cybercrime-Khadam/87d646fe076a3a5515900238555e820396bc9d2f> accessed 14 November 2023

2006. However, nobody seems to worry about it because our nation does not yet have a functioning cyber tribunal to deal with issues of this nature.

Conclusion

Bangladesh is making significant strides in achieving middle-income status. There is no way to digitally transform Bangladesh without investing in security technology, the most important aspect of which is the widespread adoption of reliable internet access. This progress calls upon ICT specialists, which we severely lack. After writing this paper, I have come to the conclusion that the state needs to be more advanced in order to detect cybercrime and, moreover, to punish the main perpetrator. This is why we need stringent restrictions or amended provisions; legal loopholes provide a safe haven for criminals. Instead of using the law as a tool of control, it should be used to establish a more just society. Another factor contributing to failure is the cops' overwhelming power. Finally, it is important to keep in mind that the nature and direction of technology are constantly shifting, necessitating the greatest possible capability on the part of the people to battle against both the real and virtual worlds to ensure the perpetual existence of a peaceful, stable and metropolitan civilization.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declarations of interest: The authors declare none.

CONFLICT OF INTEREST

The author (s) declares that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancy, have been completely observed by the authors.

OPEN ACCESS

PUBLISHER'S NOTE

REFERENCES

1. Kundu A,' Cybercrime trend in Bangladesh, an analysis and ways out to combat the threat' [2018] Electronic Journal https://www.researchgate.net/publication/324468211_Cyber_crime_trend_in_Bangladesh_an_analysis_and_ways_out_to_combat_the_threat Accessed January 2, 2023
2. Kabir SE, 'Why Are Our Digital Laws so Troublesome?' (The Daily Star, December 20 2022) <https://www.thedailystar.net/opinion/views/news/why-are-our-digital-laws-so-troublesome-3200866> accessed 1 November 2023
3. Borhanuddin, A., 2016. 'Cyber Crime and Bangladesh Perspective' Journal of Dhaka University, Department of Law, https://www.academia.edu/4488760/Cyber_Crime_and_Bangladesh_Perspective
4. Alam, A 'A New Challenge For Law Enforcers', (2004) American Journal of Public Health, 94(6 951-957. https://www.justice.gov/d9/202306/wellness_challenges_for_law_enforcement_personnel_2; Accessed November 1, 2023
5. Ahmed SM, Hossain MdM and Haque MdM, 'Usage of Facebook: Bangladesh Perspective' (SSRN, October 26, 2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2167116> Accessed November 14, 2023
6. Chen S and others, 'Exploring the Global Geography of Cybercrime and Its Driving Forces' (Nature News, February 23, 2023) < https://www.nature.com/articles/s41599-023-01560-x> accessed November 14, 2023
7. Five Factors Influencing the Cyber-security Threat Landscape' (Security Magazine RSS, August 14, 2019) <https://www.securitymagazine.com/articles/90718-five-factors-influencing-the-cybersecurity-threat-landscape> accessed December 14, 2023
8. Information And Technology Act, 2006 https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf
9. The Penal Code, 1860 http://bdlaws.minlaw.gov.bd/act-11/section-3203.html
10. Ahamed A, (2010) 'Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies' The Northern University Journal of Law, https://www. 10.3329/nujl.v1i0.18529 ISSN 2218-2578 Accessed January 10, 2023
11. Khurshid A, 'CYBERCRIME IN BANGLADESH: IMPLICATIONS AND RESPONSE STRATEGY'(2016) https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/download/82/74/149
12. Information And Technology Act, 2006 http://dohatec-ca.com.bd/DohatecCA/ICTAct.jsp
13. Mia A, (2021) 'CYBERCRIME AND ITS IMPACT IN BANGLADESH: A QUEST FOR NECESSARY LEGISLATION http://ijlljs.in/wp-content/uploads/2015/06/Cyber-Crime_Article_IJLLJS1.pdf
14. Digital Security Act, 2018 https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf
15. Why Are Cybercrimes Going Unpunished?' (The Daily Star,

August 14, 2022) < https://www.thedailystar.net/opinion/editorial/news/why-are-cybercrimes-going-unpunished-3094791> accessed December 14, 2023

16. 'Bangladesh: Cartoonist Tortured, Writer Dies in Jail: Ahmed Kabir Kishore' (Amnesty International, June 6, 2021) < https://www.amnesty.org/en/documents/asa13/3800/2021/en/> accessed December 14, 2023
17. Ahmed Q, 'Why Did Bangladesh Arrest Shahidul Alam?' (Al Jazeera, 9 August 2018) <https://www.aljazeera.com/opinions/2018/8/9/why-did-bangladesh-arrest-shahidul-alam> accessed 14 December 2023
18. Hosssain, D (2021), Bangladesh Cyber Crime Investigation and Judicial System https://www.academia.edu/4225890/Cyber_Law_Bangladesh_Perspective
19. Department K-E-KBL and others, 'Cyber Legislation and Cyber-Related Legal Issues in Bangladesh: : Inadequacies and Challenges: International Journal of Electronic Security and Digital Forensics: Vol 13, No 2' (International Journal of Electronic Security and Digital Forensics, January 1 1970) <https://dl.acm.org/doi/10.1504/ijesdf.2021.113379> accessed December 14 2023
20. Khadam A (Insight to cybercrime) <https://www.semanticscholar.org/paper/Insight-to-Cybercrime-Khadam/87d646fe076a3a5515900238555e820396bc9d2f> accessed 14 November 2023