Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview

Mohammad Shahadat Hossain[1], Mahfuza Mallika[2]

[1]Assistant Professor (adjunct), Department of Law Uttara University, Dhaka.

[2]Lecturer in CSE, Centre for General Education Bangladesh Islami University, Dhaka

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90400271

Received: 16 February 2025; Revised: 29 March 2025; Accepted: 02 April 2025; Published: 10 May 2025

ABSTRACT

Cyber security governance has become a critical component of organizational strategy in the digital era, particularly in ensuring compliance with legal and regulatory frameworks. In Bangladesh, the interplay between cyber security governance and the existing cyber laws reflects a growing need for robust mechanisms to safeguard digital infrastructure, protect sensitive information, and mitigate cyber threats. This paper provides an overview of cyber security governance within the context of the cyber laws of Bangladesh, including the Information and Communication Technology (ICT) Act, 2006, and the Cyber Security Act, 2023. It examines the legal provisions governing data protection, network security, risk management, and incident response, highlighting their alignment with global best practices. The objectives of this paper are to analyse the framework of cyber security governance in Bangladesh within the context of its existing cyber laws. It seeks to assess how these laws facilitate the implementation of cyber security measures, address challenges in governance, and align with global standards. Finally, the study presents a number of recommendations to enhance legal frameworks, strengthen institutional capacities, and promote collaboration among stakeholders to ensure a secure and resilient digital ecosystem in the country. This paper employs a qualitative doctrinal approach to analyse the ICT Act, 2006, and the Cyber Security Act, 2023, reviewing secondary sources like academic articles and legal commentaries. It conducts a comparative analysis to identify gaps and align the cyber laws of Bangladesh with global practices, proposing recommendations for improved cybersecurity governance.

Keywords: Cybersecurity governance, digital governance, cyber security act, data protection, cyber laws of Bangladesh.

INTRODUCTION

In the digital age, cyber security has become a critical concern for governments, organizations, and individuals. As reliance on digital technologies grows, so does the threat of cyber attacks, data breaches, and other malicious activities that can compromise sensitive information and disrupt critical infrastructures. Effective cyber security governance, which includes the policies, processes, and frameworks needed to manage cyber risks, is essential to safeguarding digital ecosystems and ensuring compliance with legal and regulatory standards. In Bangladesh, the rapid expansion of the digital economy and the increased adoption of online services have made cyber security governance a pressing priority. The country has enacted laws such as the Information and Communication Technology (ICT) Act, 2006, and the Cyber Security Act, 2023, to address cybercrime, regulate digital activities, and establish accountability for data protection. However, challenges remain in effectively implementing these laws due to gaps in governance, insufficient awareness, and evolving cyber threats.

Research objectives

This paper explores the landscape of cyber security governance in Bangladesh within the framework of its cyber laws. By examining the provisions of existing legislation and their alignment with international standards, the study aims to provide an overview of cyber security governance, identify challenges, and propose actionable

recommendations to enhance governance mechanisms. In doing so, it seeks to contribute to building a secure and resilient digital infrastructure in Bangladesh that aligns with global best practices.

Meaning of Cyber Security

Cyber security is the practice of protecting networks, systems, and programs from digital attacks. These attacks are typically aimed at accessing, altering, or destroying sensitive information, extorting money from users, or disrupting normal business operations. As the number of cyber-attacks continues to rise, cyber security has become an increasingly important field. It is a vital aspect of safeguarding our digital lives. Ensuring cyber security is crucial because it helps to protect data of an organization, networks, and systems from malicious attacks. It also ensures the confidentiality, integrity, and availability of data and systems of an organization. Moreover, cyber security is essential for protecting personal information, financial data, and other sensitive information from malicious actors. It also helps protect individuals from online scams, identity theft, and other forms of cyber-crime. For businesses, having robust cyber security measures in place is critical to defending their data and systems from cyberattacks. Governments also rely on cyber security to protect critical infrastructure and ensure national security.

Current Cyber Security Situation in Bangladesh

There are more than 4 billion people are now accessing in the online for variety of purposes (Kemp, 2018). The massive wave of internet and increasing dependency on online often determines our business and communication model over which we don't have control (Frangoul, 2018). On the ground of evolving digital economy, especially, during the Covid-19 and post Covid-19 business model necessarily requires strong digital security for protecting national economic growth and overall GDP of the Country (Singh, 2020). In Bangladesh, the internet users are approximately 106.410 million at the end of July, 2020 (BTRC, 2020). In 2020, Bangladesh has ranked 112 out of 121 nations in Network Readiness Index, 78th out of 100 nations in the Global Cyber security Index (NCSI), 74th National Cyber Security Index and 147th ICT Development Index (NCSI).The Government of Bangladesh started a campaign toward a vision known as "Digital Bangladesh" to make Bangladesh a digitalized country. In order to achieve the goal, all government offices have shifted from manual to digital system that necessarily requires complete dependence on internet. This massive transformation creates high probability of cyber-attack on the system that Bangladesh Government already experienced. Here is the statistical discussion on the cyber case filing ratio, trend in cyber case filing, and case completion ratio through charts and graph.

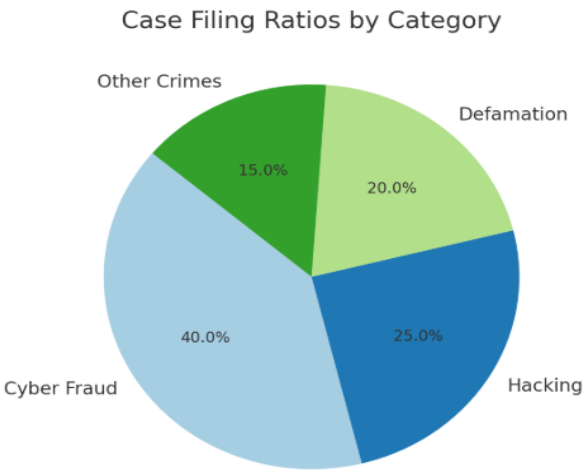

Figure 1: Case Filling Ratios by Category

According to the reports of the law enforcement agencies of Bangladesh on cybercrime case filing ratio expressed in the chart. The chart on case filing ratios categorizes of cybercrime incidents in Bangladesh, with cyber fraud accounting for the largest share (40%), followed by hacking (25%), defamation (20%), and other crimes (15%). This distribution reflects the growing financial and security threats posed by online fraud and hacking, which are increasingly reported under the ICT and Cyber Security Act. The lower proportion of

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue IV April 2025

defamation and other crimes suggests that while digital harassment and misinformation are significant issues, they may be underreported or less frequently prosecuted.

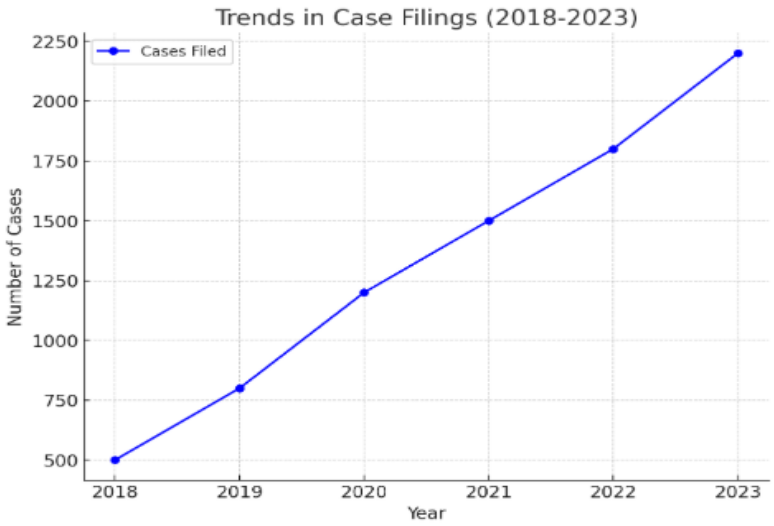

Figure 2: Trends in Case Filing (2018-2023)

In addition, the line graph illustrates a continuous rise in cyber case filings in Bangladesh, increasing from 500 in 2018 to 2,200 in 2023, indicating a growing awareness and reporting of cybercrimes. This upward trend reflects the rapid digitalization of financial transactions, social media usage, and online activities, leading to more cyber-related offenses. The sharp increase also highlights the need for stronger legal frameworks, better enforcement mechanisms, and enhanced cyber security measures to manage the surge in cybercrime cases effectively.

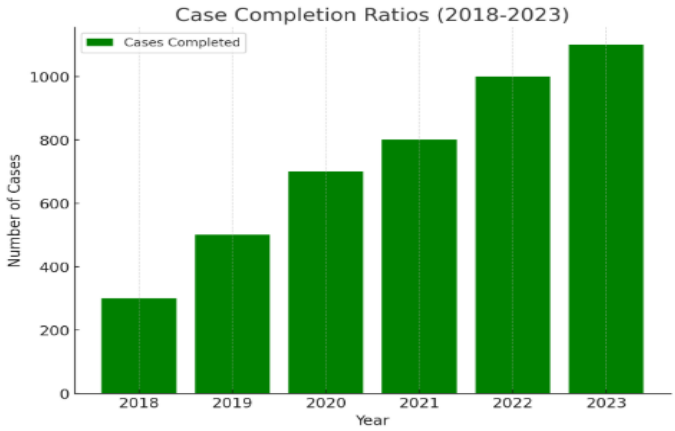

Figure 3: Case Filing Ratios (2018-2023)

Furthermore, the bar chart reveals a persistent gap between the number of cyber cases filed and those resolved each year, with completion rates lagging behind the rising trend in filings. Although case resolutions increased from 300 in 2018 to 1,100 in 2023, the backlog remains significant, indicating delays due to legal complexities, resource constraints, and investigative challenges. This disparity emphasizes the need for judicial reforms, specialized cybercrime units, and streamlined legal procedures to improve case resolution efficiency.

Therefore, like other South Asian countries, the government of Bangladesh is facing complex multifaceted cyber security threats that cause or might cause potential damage to the national economic growth (CSCR Bangladesh, 2018). To address this issue, Government started to develop a legal framework for cyber security and enacted the law known as “Information and Communication Technology Act 2006”. But the law was insufficient in terms of addressing digital security and data protection concerns (e-Government Master Plan for Digital Bangladesh, 2018). Thus, Government has taken steps to develop its digital security framework through its e-governance project and “Digital Bangladesh” vision (NCSS Bangladesh, 2014). In addition, the government

prepared a National Cyber security Strategy, charting a vision for cyber security till 2021(Aguilera et al., 2020). Furthermore, in order to boost the digital data security, Government has taken further step and legislated a new law known as "Digital Security Act, 2018 which was subsequently repealed and another new piece of law was enacted known as Cyber Security Act, 2023.

Furthermore, Bangladesh and many other developing nations move towards the digital transformation to develop the Health and Telemedicine in our private and public hospitals. It has many witnessed a rapid increase of digital health amenities, including: Telemedicine platforms like Praava Health, Doctorola, and Tonic, Electronic medical record (EMR) systems in private hospitals, Government initiatives like Shastho Batayon (16263) for remote healthcare, AI-driven diagnostics and smart health devices. But this develop will not be continue without Cyber Security in Bangladesh. Some challenges in Bangladesh's Healthcare Sector are Weak or Non-Existent Regulations, Unsecured Digital Health Records, Poor Cyber Hygiene, Growing Cyber Threats, Lack of Incident Response (Rumi, 30 January, 2025).

Moreover, Human rights for freedom of expression have some threats. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantees the right to freedom of opinion and expression, as well as the right to receive and impart information and ideas. It includes 'political discourse, remarks on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. Section 57 of the ICT Act contravenes Bangladesh's obligations under Article 19 of the ICCPR: the offences arranged are unclear and the restrictions compulsory on freedom of opinion and expression in Bangladesh (ICJ, 2013).

Cyber Laws of Bangladesh: At a Glance

In order to prevent and control cybercrime, the Government of Bangladesh has passed several laws and regulations, including the Information and Communication Technology (ICT) Act, 2006, as amended in 2008, 2009, and 2013; the Digital Security Act, 2018 (now repealed); and the newly enacted Cyber Security Act, 2023. Additionally, the Information Technology (Certificate Authority) Rules, 2010, and the Cyber Security Rules, 2024, are key regulations for addressing cyber security and cybercrimes in Bangladesh. These laws form the primary legal framework for tackling cybercrime. Other laws also intersect with anti-cybercrime efforts, such as the Code of Criminal Procedure, 1898, the Penal Code**,** 1860**,** the Evidence Act, 1872**,** the Contract Act, 1872**,** the Banker's Books Evidence Act, 1891**,** the Crime Related Interpersonal Assistance Act, 2012, the Right to Information Act, 2009**,** and the Official Secrets Act, 1923.To counter the growing cybercrime issue in Bangladesh, experts recommend amending several laws, including the Code of Criminal Procedure, 1898**,** the Penal Code, 1860**,** the Evidence Act, 1872**,** and the Contract Act, 1872**.** Furthermore, the Honourable High Court Division of the Bangladesh Supreme Court has provided guidelines for bail hearings under the ICT Act, 2006, in the case of *Md Sabuj Ahmad vs State*in 2017.

The ICT Act, 2006, while pioneering in establishing a legal framework for cybercrimes in Bangladesh, has faced significant challenges in implementation, limiting its effectiveness. A key issue lies in the lack of technical expertise among law enforcement and judiciary officials, leading to inefficient enforcement and case backlog. The ambiguous wording of provisions, particularly Section 57, has resulted in misuse and raised concerns over freedom of expression. Additionally, inadequate infrastructure and overlapping legal frameworks, especially with the Digital Security Act (DSA), 2018 subsequently repelled, have created confusion and inefficiencies. Despite its role in increasing cybercrime awareness and legalizing digital transactions, the Act struggles to keep pace with evolving cyber threats like ransomware and deep fake technology. To enhance its effectiveness, Bangladesh must modernize its legal framework, invest in cyber security training, and establish clearer legal provisions to balance digital security and civil rights (Badruzzaman, M.,2016).

On the other hand, the Cyber Security Act (CSA) of 2023, while ostensibly aimed at strengthening cyber security frame work in Bangladesh, has been widely criticized for retaining the repressive elements of its predecessor, the Digital Security Act (DSA) of 2018. Despite claims of reform, the Act continues to raise concerns about the suppression of freedom of expression, as noted by Amnesty International, which argues that it merely recycles problematic provisions (Amnesty International, Bangladesh, August 8, 2024). Furthermore, its vague definitions and broad enforcement powers grant authorities unchecked discretion, increasing the risk of arbitrary arrests and

media censorship, as highlighted by the Editors' Council (Dhaka Tribune, 20 Sep 2023). This ambiguity, coupled with the potential for misuse against journalists and dissenting voices, as Transparency International Bangladesh warns and suggests that the Act may be more focused on controlling digital discourse than genuinely addressing cyber threats. The lack of clear safeguards against legal harassment and the continued erosion of press freedom cast doubt on the Act's effectiveness in fostering a secure yet open digital environment, making it more of a political tool than a cyber security measure (Cyber Security Act-2023, Aug 30, 2023).

Definition of Cyber Security Governance

Cyber Security governance refers to the system by which an organization directs and controls its approach to cyber security, ensuring alignment with its objectives, compliance with regulations, and effective risk mitigation. It encompasses policies, procedures, and oversight mechanisms for managing cyber security risks, with key components including strategic alignment with organizational goals, risk management to protect critical assets, policy development for guiding behaviour, compliance oversight with laws and standards, and an accountability framework defining roles and responsibilities. Effective cybersecurity governance is vital to both corporate and IT governance, providing the structure for setting objectives, monitoring performance and managing risks (Aguilera et al., 2020). It integrates accountability frameworks, compliance monitoring, and strategic alignment, enabling organizations to proactively manage evolving cyber threats. The objectives of cyber security governance include establishing a structured framework to manage and mitigate cyber risks, ensuring alignment with organizational goals, compliance with legal and regulatory requirements and the protection of information assets. This involves defining clear policies and procedures, assigning responsibilities, and implementing oversight mechanisms to safeguard against cyber threats. Effective cyber security governance also aims to foster a culture of security awareness and continuous improvement within the organization (Alotaibi etal, 2021). A well-structured cyber security governance framework enables organizations to detect, prevent, and respond to cyber incidents, thereby reducing risk exposure and supporting informed decision-making.

Components of Cyber Security Governance and Cyber Laws in Bangladesh

Cyber Security governance refers to the framework and practices that ensure the protection of an organization's digital assets, compliance with legal and regulatory requirements, and alignment with business objectives. The key components of cybersecurity governance are outlined below:

Risk Management

Risk management in cyber security governance involves identifying, assessing, and mitigating risks associated with cyber threats to ensure business continuity and minimize potential damage. The risk assessment process includes identifying vulnerabilities, threats, and the likelihood of exploitation. On the other hand**,** risk mitigation involves implementing controls such as firewalls, intrusion detection systems, and employee training, while risk monitoring entails continuously monitoring risks and updating mitigation strategies as threats evolve (Smith et al. 2022). In Bangladesh, the ICT Act, 2006 primarily focuses on preventing cybercrimes and establishing accountability in digital transactions. It addresses aspects of risk management indirectly through provisions related to securing digital systems and punishing cybercriminal activities. The ICT Act, 2006 collectively addresses risk management by emphasizing preventive measures against cyber threats. It penalizes unauthorized access to computer systems, highlighting the need for risk mitigation strategies such as access controls and intrusion prevention (S 54, ICT Act, 2006). The Act further criminalizes hacking, encouraging organizations to adopt robust risk assessment tools and monitoring systems to detect and deter such activities (S 56, ICT Act, 2006). Similarly, the law imposes liability for the negligent protection of sensitive information, prompting the use of encryption, data backups, and other safeguards to minimize risks (S 63, ICT Act, 2006).

The Cyber Security Act, 2023 (CSA) of Bangladesh introduces several provisions pertinent to risk management in cybersecurity governance. The Act collectively emphasizes the integration of risk management within the cybersecurity governance framework in Bangladesh. It mandates the establishment of the National Cyber Security Agency (NCSA**)** to oversee and implement nationwide cyber security measures (S 5, Cyber Security Act, 2023). While Section 6 outlines the appointment of its leadership, highlighting the importance of specialized expertise for effective governance and compliance (S 6, Cyber Security Act, 2023). The law empowers the

NCSA to proactively mitigate risks by removing or blocking data that poses cyber threats but has faced criticism for prioritizing punitive actions over continuous risk management and resilience-building (S 8, Cyber Security Act, 2023). Additionally, it raises concerns about balancing national security with individual rights, reflecting ongoing debates about the broader implications of the Act for governance (Khan et al, 2023).

Furthermore, the Act establishes the National Cyber Security Council (NCSC) as the apex body for cyber security governance under Section 4, tasked with developing and approving national policies, ensuring alignment with global best practices, and addressing emerging threats. The Act entrusts the NCSC with coordinating efforts among government bodies, private entities, and international stakeholders, mandates monitoring policy implementation, and reviewing the performance of agencies like the NCSA (S 4(b), (c), Cyber Security Act, 2023). Additionally, it assigns the NCSC responsibility for managing national-level responses to major cyber incidents, focusing on capacity building, research, and public awareness initiatives NCSA (S 4(d), (e), Cyber Security Act, 2023). The NCSC plays a critical role in bridging policy-making with implementation, though its success depends on resources, collaboration, and adaptability to evolving cyber risks.

Incident Response

Incident response refers to the structured approach to identifying, managing, and mitigating the effects of cyber incidents, such as data breaches or malware attacks (Rodriguezet et al., 2023). Incident response under the cyber laws of Bangladesh is primarily addressed through the ICT Act, 2006 and the Cyber Security Act, 2023**,** which establish frameworks for handling cyber incidents, including data breaches, hacking, and cybercrime. The ICT Act, 2006 addresses incident response through provisions related to risk management as mentioned above. These sections criminalize unauthorized access to computer systems, enabling legal action against intruders, penalize hacking and data manipulation, facilitate law enforcement response to hacking incidents, and hold organizations accountable for failing to protect sensitive information, thus triggering responses in cases of data breaches (S 54,56,63, The ICT Act 2006). On the other hand, the Cyber Security Act**,** 2023 outlines incident response through Section 4(d)**,** which assigns the National Cyber Security Council (NCSC) the responsibility of managing national-level responses to major cyber incidents, ensuring coordinated action during security breaches. The Act empowers the National Cyber Security Agency (NCSA) to take corrective measures, such as blocking harmful data, to mitigate risks. Together, these provisions combine legal penalties and proactive measures for effective cyber incident management (S 8, Cyber Security Act, 2023).

Security Awareness

Security awareness involves educating employees and stakeholders about cyber threats, safe practices, and their role in maintaining organizational security. It encompasses training programs such as workshops and simulations to improve cyber hygiene, phishing campaigns to test employee awareness through simulated phishing emails, and continuous engagement, including regular updates and resources to keep employees informed about emerging threats (Nguyen et. al, 2021). Under the ICT Act, 2006, security awareness is indirectly addressed through provisions emphasizing the protection of systems and data. Sections 54 and 56 of the Act imply the need for security awareness, while Section 66 penalizes actions that compromise the security of information and communication systems, underscoring the importance of understanding and safeguarding against cyber risks (S 66, The ICT Act 2006). Although the Act does not explicitly focus on awareness campaigns, it establishes a legal framework that encourages proactive security practices. The Cyber Security Act, 2023, explicitly emphasizes security awareness through Section 4(e), mandating the National Cyber Security Centre (NCSC) to promote capacity building and awareness about cyber risks among individuals and organizations (S 4(e), Cyber Security Act, 2023). This provision highlights the critical role of education and training in preventing cyber incidents (S 8, Cyber Security Act, 2023). Together, these provisions stress the importance of continuous education and a proactive approach to mitigating emerging cyber threats (Bashar et al., 2023).

Network Security

Network security involves safeguarding an organization's IT infrastructure from unauthorized access, misuse, and disruptions. The key elements of network security include Firewalls (Controlling network traffic based on security policies), Intrusion Detection and Prevention Systems (Monitoring for and responding to network-based

threats), Virtual Private Networks (Ensuring secure remote access), Network Segmentation (Dividing networks to limit lateral movement during breaches) (Kumar et al. 2023). In Bangladesh, network security is addressed through the ICT Act, 2006 and the Cyber Security Act, 2023, with provisions focusing on the protection of systems and critical infrastructure.

The ICT Act, 2006 criminalizes unauthorized access (Section 54), penalizes hacking activities (Section 56), and targets actions that compromise communication systems (Section 66).

The Cyber Security Act, 2023 assigns the National Cyber Security Centre (NCSC) to oversee national-level responses to cyber incidents (Section 4(d)) and empowers the National Cyber Security Authority (NCSA) to block harmful data that affects network security (Section 8).

Together, these laws establish robust frameworks for preventing unauthorized access and mitigating cyber threats.

Data Protection

Data protection encompasses measures to ensure the confidentiality, integrity, and availability of organizational data. The key components of data protection include Data Encryption (Encoding sensitive information to prevent unauthorized access), Access Controls (Restricting data access based on roles and responsibilities), Data Loss Prevention **(**Implementing tools to monitor and protect data from leaks), Compliance (Adhering to relevant regulations) (Taylor et al, 2023). In Bangladesh, data protection under the ICT Act, 2006 and the Cyber Security Act, 2023 aims to safeguard personal and sensitive information from unauthorized access, misuse, and breaches. These laws provide a framework for data protection by criminalizing unauthorized access, ensuring accountability for data security, and empowering authorities to take preventive and corrective actions to protect sensitive information (Rahman et al. 2023). While both Acts address data protection, the Cyber Security Act, 2023, offers a more comprehensive and coordinated approach. The ICT Act, 2006, primarily focuses on legal penalties for breaches. The **Cyber Security Act, 2023**, builds on the foundation laid by the ICT Act by providing a proactive, organizational, and national-level framework for securing data and critical infrastructure (Ahmed, 2022).

Cyber Security Governance in Cyber Laws of Bangladesh

Cyber Security Management in Bangladesh is addressed by two primary cyber laws: the Information and Communication Technology (ICT) Act, 2006**,** and the Cyber Security Act, 2023. This section analyses the management aspects of cyber security under these two laws in chronological order.

Information and Communication Technology Act of 2006 (The ICT Act (Act No. 39), 2006)

The Information and Communication Technology Act of 2006 (ICT Act 2006**)** is a law regulating the use of information and communication technologies (ICTs) in Bangladesh. Passed by the Parliament of Bangladesh in 2006, the Act aimed to promote the use of ICTs, protect citizens' rights, and establish a legal framework for regulating the ICT sector. The ICT Act 2006 has been instrumental in enabling Bangladesh to progress toward a more digitally enabled society by providing a legal foundation for ICT Governance. The Act is divided into nine parts, with Parts V and VIII addressing aspects of cybersecurity governance. Part V: Focuses on provisions for controllers and certifying authorities, including foreign certifying authorities. It outlines their powers, functions, and duties concerning Digital Signature Certificates (DSCs). Part VIII: Includes Chapters 2 and 3, which provide for the establishment of the Cyber Tribunal and Cyber Appellate Tribunal to address breaches of the Act's provisions. The ICT Act of 2006 was a pivotal legislative measure aimed at establishing legal recognition and security for electronic transactions and regulating cyber activities in Bangladesh. Its primary objectives included: promoting the growth of the information technology sector, ensuring the security of electronic records and digital signatures, combating cybercrimes. A significant aspect of the ICT Act was its emphasis on cybersecurity governance. It established a legal framework to address cyber offenses, including hacking, unauthorized access to computer systems, and the dissemination of obscene or defamatory content online.

Cyber Security Governance under the Controller and Certifying Authorities:

The ICT Act, 2006 defines a Controller, Deputy Controller, or Assistant Controller as a person appointed by the government through a notification in the official gazette within 90 days of the enactment of the Act (S 18 (1-4), Ibid). These individuals must meet the qualifications specified by the service code and perform the functions outlined in the Act. The Act further defines a Certifying Authority (CA) as a person or entity granted a license under Section 18, read in conjunction with Section 22 of the Act, to issue Digital Signature Certificates (DSCs**)** (S 2(32), The ICT Act 2006). The ICT Act, 2006, established the Controller of Certifying Authorities (CCA) to regulate digital signatures and ensure cyber security. The CCA is responsible for overseeing certifying authorities, which are licensed entities tasked with issuing, renewing, and revoking digital signature certificates. These certificates are critical for securing electronic transactions by ensuring Authentication (Verifying the identity of parties involved), Data Integrity (Ensuring that data remains unaltered during transmission), Non-repudiation (Preventing denial of involvement in a transaction). The CCA ensures that certifying authorities comply with regulations, maintain secure infrastructure and adhere to international cryptographic standards (Chowdhury et. al, 2021). The role of the Controller of Certifying Authorities **(CCA)** in cyber security governance under the ICT Act, 2006, is outlined as follows:

Appointment of the Controller and Staff

The ICT Act specifies the government responsibility for appointing the Controller**,** along with Deputy Controllers and Assistant Controllers**;** to manage and oversee the operations of Certifying Authorities (CAs) (S 18(1), The ICT Act.2006**).** This provision establishes a regulatory framework to ensure the effective supervision of CAs, which are responsible for issuing Digital Signature Certificates (DSCs**)** and maintaining the security and integrity of digital transactions. The Controller plays a central role in regulating the operations of Certifying Authorities. CAs is authorized entities tasked with issuing DSCs to authenticate and secure digital communications. As the head of this regulatory system, the Controller holds supervisory responsibility to ensure that all CAs adhere to the standards and regulations outlined in the ICT Act**.**

Supervision and Standards for Certifying Authorities

The ICT Act defines the responsibilities of the Controller to supervise Certifying Authorities **(CAs)** and establish the standards they must follow. The Controller ensures that CAs operate in compliance with legal and technical regulations, particularly regarding the issuance of Digital Signature Certificates (DSCs)**,** to maintain their integrity and security. By overseeing the activities of CAs, the Controller ensures that they adhere to prescribed operational, security, and technical standards, which are essential for safeguarding the reliability of digital signatures in transactions. This supervision helps prevent misuse or fraudulent activities, fostering a secure and trustworthy digital environment (Sections 19(a) and 19(b), The ICT Act, 2006).

Licensing and Qualifications of Certifying Authorities

The ICT Act outlines the role of the Controller in granting licenses to Certifying Authorities (CAs) and specifying the qualifications required for their employees. The Controller ensures that only qualified entities are authorized to issue Digital Signature Certificates (DSCs)**,** thereby safeguarding the integrity of the certification process. Additionally, by setting specific qualification requirements for CA staff, the Controller ensures that personnel possess the necessary technical expertise to manage and secure digital signature operations. This helps maintain high standards of cyber security and fosters trust in digital transactions (Sections 22(1) and 19(c), The ICT Act, 2006).

Investigation and Enforcement

The ICT Act grants the Controller the authority to investigate violations and access computer systems if non-compliance with the Act is suspected. This investigative power enables the Controller to address any contraventions, ensuring that Certifying Authorities and entities involved in digital signature issuance adhere to legal and security standards (S 29 and 30, The ICT Act, 2006). By conducting investigations and accessing

relevant systems, the Controller plays a crucial role in maintaining the integrity and security of digital signatures in the country.

Digital Signature Repository and Publication of Revocation

The ICT Act outlines the responsibility of the Controller to maintain a secure repository of all issued Digital Signature Certificates (DSCs) and to publicly notify any revocations or suspensions (S 29 and 30, Act No. 39 of the year 2006). By acting as the central repository, the Controller ensures the integrity and accessibility of digital signatures. The publication of revocations further promotes transparency and trust in the digital certification process, helping prevent misuse and ensuring the credibility of digital transactions.

Establishment of Cyber Tribunal

The Government shall establish one or more Cyber Tribunals in consultation with the Supreme Court and appoint a Judge to be known as "Judge, Cyber Tribunal" under this Act. The purpose of the Tribunal is to conduct effective trials of offenses. The local jurisdiction of the Cyber Tribunal can cover all of Bangladesh or one or more Session Divisions, to prosecute offenses committed under this Act. Ongoing prosecutions or cases in any Session Court shall not be automatically suspended or transferred to the Cyber Tribunal due to the jurisdictional changes, unless the concerned Tribunal of local jurisdiction is involved. The Government may transfer cases to the Tribunal with special local jurisdiction by issuing a notification in the Official Gazette. The Cyber Tribunal shall make decisions on prosecutions based on statements already taken from witnesses and is not required to retake statements, conduct rehearing, or perform other activities to execute the prosecution. The Government shall define the place and time according to the special activities of the Tribunal. The role of the Tribunal is outlined below:

Adjudication of Cybercrime Cases: Under Section 68 of the ICT Act, 2006**,** the Cyber Tribunal is responsible for adjudicating cases related to offenses under the Act, including cybercrimes. These offenses may involve unauthorized access to computer systems, data theft, cyber fraud, and other digital crimes. The Tribunal ensures that individuals or entities engaged in illegal activities in cyberspace are held accountable under the law. It interprets and applies legal provisions concerning cyber security breaches, making it a crucial component of the legal framework for managing and regulating digital activities.

Imposition of Penalties: The Cyber Tribunal has the authority to impose penalties for various violations, including cybercrimes and non-compliance with regulations related to digital signatures, data protection, and other cyber security provisions. The Tribunal can impose fines, and in more severe cases, award imprisonment, ensuring that offenders are held legally accountable. This authority helps deter illegal activities in the digital domain, upholds the integrity of the Act, and ensures the protection of individuals, organizations, and the nation's cyber security infrastructure.

Interpretation and Legal Consistency: The ICT Act, 2006 grants the Cyber Tribunal the responsibility of interpreting the provisions of the Act. This role is crucial in ensuring uniformity and consistency in how the law is applied across various causes related to cyber security. By offering authoritative interpretations, the Tribunal helps create a clear legal framework, guiding authorities and stakeholders in resolving disputes and addressing complex issues related to digital offenses, data protection, and cyber security governance. This contributes to maintaining legal clarity and consistency in enforcing the law.

Establishment of Cyber Appellate Tribunal and the Cyber Security Governance

The Government shall establish one or more Cyber Appellate Tribunals**,** known as the Appellate Tribunal. The Appellate Tribunal shall consist of one Chairman and two members**,** all to be appointed by the Government. A person shall not be qualified to serve as the Chairman of the Cyber Appellate Tribunal unless they are qualified to be a Judge of the Supreme Court**.** One of the members shall be serving in the judicial department or be a retired District Judge, and the other member shall have adequate knowledge and experience in Information and Communication Technology (ICT)**.** The Chairman and two members shall serve terms ranging from 2 to 5 years**,** as determined by the Government, with the terms of reference also set by the Government.

Cyber Security Act of 2023

Cyber Security Agency in Cyber Security Governance

Establishment of Cyber Security Agency

The Government shall establish an agency known as the National Cyber Security Agency**,** consisting of one Director and additional Directors as specified by rules in the official Gazette. The Director General and the Directors will be appointed by the Government from among specialists in computer science or cyber security. The Agency's headquarters will be located in Dhaka**,** with additional branch offices established outside Dhaka within the country. Administratively, the Agency will be affiliated with the Information and Communication Technology Division**.** The powers, responsibilities, and functions of the Agency will be defined by rules.

Role of the Cyber Security Agency in Cyber security Governance

The Cyber Security Agency under the Cyber Security Act of 2023 plays a central role in protecting the nation's digital infrastructure and ensuring the overall security of cyberspace. Established by the Act, the Agency is responsible for implementing and overseeing national cyber security strategies, policies, and programs. It coordinates with government entities, private organizations, and international bodies to address emerging cyber threats and vulnerabilities. The Agency's key functions include developing cybersecurity frameworks, monitoring cyber threats, providing guidance on best practices, conducting cybersecurity awareness campaigns, and coordinating incident response efforts. It also works on the enforcement of security regulations and standards, aiming to mitigate risks and promote the resilience of critical digital infrastructure against cyberattacks. The **Cyber Security Agency** serves as a key body in fostering collaboration across sectors, enhancing the nation's readiness to combat cybercrime, and ensuring a secure digital environment.

Cyber Security Council in Cyber Security Governance

Establishment of Cyber Security Council

The Cyber Security Council, established under the Cyber Security Act of 2023**,** play**s** a crucial role in providing strategic guidance and oversight on national cybersecurity matters. It is responsible for formulating national cyber security strategies, establishing governance frameworks, and advising the government on cyber security challenges (Act No. 39 of the year 2006). The Council ensures a coordinated approach to managing cyber threats, fostering collaboration across government, private sectors, and other stakeholders. It oversees the implementation of cyber security programs, aligns them with national security goals, and ensures they meet international standards. Additionally, the Council coordinates critical infrastructure protection, responds to emerging threats, promotes public awareness, and encourages the development of a skilled cybersecurity workforce. The goal is to create a secure digital environment that supports economic growth and safeguards national interests.

Role of the Cyber Security Council in Cyber Security Governance

The Cyber Security Council**,** established under the Cyber Security Act of 2023**,** plays a critical role in shaping and overseeing the country's cyber security governance. It is responsible for formulating national cyber security strategies, advising the government on key cyber security issues, and ensuring the alignment of cyber security policies with national security objectives. The Council coordinates efforts across government agencies, private sectors, and international partners to address cyber threats, protect critical infrastructure, and enhance the country's resilience to cyberattacks. Additionally, it promotes public awareness, fosters the development of a skilled cyber security workforce, and ensures that the country's cyber security framework is continuously updated to address emerging risks and challenges.

Global Alignment and the Position of Bangladesh : Bangladesh is progressively aligning its cybersecurity governance with global standards by actively participating in international cybersecurity initiatives and adopting ISO/IEC 27001 for information security management. The country collaborates with global organizations such

as the Forum of Incident Response and Security Teams (FIRST) and the Asia Pacific Computer Emergency Response Team (APCERT) to strengthen its cybersecurity framework, enhance incident response capabilities, and stay informed on emerging threats. Bangladesh also engages with the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI), where it has improved its ranking but still trails behind leading cybersecurity nations. Furthermore, financial institutions and government agencies in Bangladesh have started implementing ISO/IEC 27001 to enhance information security management. Despite these advancements, challenges such as limited skilled professionals, regulatory gaps, and the high cost of certification remain. To strengthen its cybersecurity posture, Bangladesh must continue fostering international partnerships, enforcing mandatory cybersecurity standards, and investing in capacity-building initiatives (Uddin, M. R., 2021).

Similarly, Bangladesh is adopting ISO/IEC 27001, the international standard for information security management, to enhance cybersecurity resilience across various sectors. Financial institutions, particularly banks, are implementing ISO/IEC 27001 to safeguard digital banking infrastructure and comply with Bangladesh Bank's cybersecurity mandates. Government agencies such as BGD e-Gov CIRT and the Bangladesh Computer Council (BCC) are also integrating this standard to protect critical state-level digital assets. In the private sector, major telecom, IT, and e-commerce companies are adopting ISO/IEC 27001 to gain credibility in global markets, driven in part by multinational corporations requiring compliance from local partners. However, challenges such as high certification costs, a shortage of skilled professionals, regulatory gaps, and limited awareness hinder widespread adoption. To accelerate implementation, Bangladesh must offer financial incentives, expand cybersecurity training programs, enforce mandatory compliance for critical sectors, and launch awareness campaigns to promote the importance of ISO/IEC 27001 in securing the nation's digital infrastructure (Pushpo & Uddin, 2022).

Challenges of Cyber Security Governance in Bangladesh

Cyber security governance in Bangladesh faces multifaceted challenges amid rapid digital transformation. These challenges arise from an evolving digital landscape, underdeveloped infrastructure, and global cyber threats. Addressing these challenges requires strategic policies, robust technology, and capacity building. Below is an analysis of the key challenges:

Implementation Challenges of the ICT ACT

Lack of Technical Expertise: Many law enforcement agencies and judicial officials lack the necessary technical knowledge to properly interpret and enforce cyber laws, leading to delays and inefficiencies in legal proceedings.

Ambiguity in Legal Provisions: Certain provisions in the ICT Act, such as Section 57, have been criticized for their broad and vague wording, making them susceptible to misuse and misinterpretation.

Inadequate Infrastructure: The absence of advanced forensic tools and trained cybercrime investigators limits the government's ability to efficiently track and prosecute cybercriminals.

Delays in Case Resolution: The backlog of pending cyber cases due to lengthy legal procedures and administrative inefficiencies reduces the Act's deterrent effect.

Overlapping with Other Laws: The introduction of the Digital Security Act (DSA), 2018, has led to conflicts and redundancies, creating confusion over which law applies in specific cases.

Implementation Challenges of the CSA ACT

Retention of Controversial Provisions: The CSA retains many provisions from the DSA that have been criticized for suppressing freedom of expression. Amnesty International notes that the CSA "rehashes almost all of the repressive provisions of the repealed Digital Security Act (DSA) 2018," leading to concerns about continued suppression of dissent.

Vague Definitions and Broad Powers: The Act grants authorities extensive powers to search, arrest, and detain individuals without clear safeguards. The Editors' Council has expressed concern that the CSA contains elements that erode freedom of speech and media freedom, highlighting the need for clearer definitions to prevent misuse.

Potential for Misuse: There is apprehension that the CSA could be used to target journalists and suppress press freedom. Transparency International Bangladesh (TIB) has rejected the Act, stating that it includes controversial sections of the DSA and could lead to the continuation of restrictions on freedom of speech and the press. Critics argue that the Cyber Security Act (CSA) retains key elements of the now-repealed Digital Security Act (DSA), which had been widely condemned for being used to criminalize dissent, harass journalists, and silence activists. TIB and other rights organizations have pointed out that vague and broadly defined provisions in the CSA could be exploited to prosecute individuals for legitimate journalistic work or criticism of the government. The law's provisions on defamation and misinformation, they argue, can be used selectively to suppress investigative reporting and public discourse on matters of national interest. Furthermore, past instances of the DSA being used to detain journalists, restrict access to information, and intimidate dissenting voices raise concerns that the CSA may serve as a continuation of these practices. While the government maintains that the CSA is intended to strengthen cybersecurity and combat digital crimes, transparency advocates stress the need for safeguards to prevent its misuse against journalists and media professionals (TIB, Cyber Protection Ordinance 2024).

Prevalence of Cyber Threats

Bangladesh regularly encounters cyber threats such as malware, phishing attacks, data breaches, and financial scams. These threats target government agencies, businesses, and individuals, resulting in significant data breaches and financial losses (Section 12,13). For example, the 2016 Bangladesh Bank heist exposed vulnerabilities in the country's financial cybersecurity.

Inadequate Cyber Security Infrastructure: The country's cyber security infrastructure remains underdeveloped, lacking advanced threat detection and response mechanisms. This inadequacy hampers the ability to effectively counter cyber threats. Outdated systems limit proactive measures against sophisticated cyber-attacks, leaving critical sectors vulnerable.

Legal and Policy Challenges: The evolution of cyber laws in Bangladesh has been contentious. The Information and Communication Technology (ICT) Act, 2006**,** and its amendment in 2013 faced criticism for vague provisions that potentially suppressed freedom of speech. The Digital Security Act, 2018**,** which replaced the ICT Act, was also controversial and eventually repealed in 2023, replaced by the Cyber Security Act, 2023. While the Digital Security Act aimed to strengthen cyber law, it faced criticism for its misuse in suppressing freedom. The new Cyber Security Act, 2023, needs effective implementation to balance enforcement with individual rights.

Data Breaches: Data breaches have become a significant cybersecurity issue in Bangladesh. In 2023, a major breach exposed the personal data; including the national ID numbers of over 50 million citizens, due to vulnerabilities in government websites (Syed Shadman Wahid, 2024). The frequency and scale of these breaches underline the urgent need for improved data protection measures and cybersecurity governance. A comprehensive approach combining legal reforms, technological upgrades, and public-private collaboration is essential to mitigate risks. Without these measures, Bangladesh's digital transformation will continue to face challenges in ensuring data security and maintaining public trust (Billah et al., 2023).

Inadequate Cyber Security Expertise: The shortage of skilled cyber security professionals is one of the critical impediments to developing robust cyber security frameworks in Bangladesh. This gap undermines efforts to counter cyber threats, develop effective incident response mechanisms, and maintain secure digital infrastructure (Nabi, 2014). Bangladesh faces a significant shortage of cyber security expertise due to limited specialized education and training programs, with local IT curricula focusing more on general computer science than cyber security. Brain drain exacerbates the issue, as skilled professionals seek better opportunities abroad. Low awareness among decision-makers leads to underinvestment in cyber security training, while rapid advancements in cyber threats outpace local skill development. High costs for globally recognized certifications

and insufficient collaboration with international experts further hinder capacity building, leaving the country vulnerable to evolving cyber challenges (Sarker et al.,2024).

Low Public Awareness: Low public awareness is a critical challenge in strengthening cyber security in Bangladesh. Many citizens lack knowledge about basic digital safety practices, such as using strong passwords, avoiding phishing scams, and protecting sensitive information online. This knowledge gap increases vulnerabilities, making individuals and organizations easy targets for cybercriminals. Additionally, there is limited public understanding of risks associated with data breaches, ransomware, and other threats, which hampers proactive measures. The absence of widespread awareness campaigns and educational initiatives exacerbates the problem, underlining the need for targeted efforts to promote cyber security literacy across all segments of society (Mamun et al., 2021).

Challenges in Critical Sectors: Challenges in critical sectors such as finance, healthcare, and energy significantly hinder Bangladesh's cyber security landscape. Financial institutions, frequently targeted by cybercriminals, face risks like data breaches and fraudulent transactions, as seen in high-profile incidents like the Bangladesh Bank heist. Healthcare systems, increasingly digitized, are vulnerable to ransomware attacks, risking sensitive patient data and service disruptions. The energy sector, vital for national infrastructure, faces threats from sophisticated state-sponsored attacks aimed at destabilizing critical operations. These challenges are exacerbated by outdated systems, inadequate security protocols, and insufficient skilled personnel. Addressing these vulnerabilities requires sector-specific strategies, investments in modern technologies, and enhanced coordination among stakeholders to safeguard critical assets (Sarker et al., 2024).

Strengthen Cyber Security Governance in Bangladesh:

To strengthen cybersecurity governance in Bangladesh, a balanced approach combining legal frameworks, technical solutions, and workforce development is crucial.

Data Protection Strategies: Bangladesh should adopt comprehensive data protection laws aligned with international standards like the General Data Protection Regulation (GDPR). Strengthening legal frameworks around data privacy, along with implementing encryption and access controls, will ensure sensitive data remains secure from breaches.

Workforce Development: Building a skilled cybersecurity workforce is essential. Bangladesh must invest in education and training programs to produce certified cybersecurity professionals. Collaboration with global organizations for knowledge-sharing and conducting cybersecurity awareness programs for businesses and government agencies will also be critical.

Integrating Technical Solutions: Implementing technical solutions such as firewalls, intrusion detection systems (IDS), and advanced threat protection tools can bolster Bangladesh’s cybersecurity posture. These should complement the legal and regulatory frameworks by enabling proactive threat monitoring and incident response capabilities. By integrating these strategies, Bangladesh can establish a practical and robust cybersecurity framework that balances legal, technical, and human resource aspects effectively.

Recommendations: Based on the challenges discussed above, the study offers several recommendations which are as follows:

Strengthening Legal and Regulatory Frameworks: Implementing comprehensive cyber security laws that balance state interests and individual rights is essential.

Enhancing Cyber security Infrastructure: Investing in modern technologies for advanced threat detection and mitigation is crucial.

Focus on Content Regulation over Security Measures: The Act appears more focused on regulating digital content than on implementing robust cyber security measures. This focus may divert attention from developing comprehensive strategies to combat genuine cyber threats.

Erosion of Public Trust: The perceived continuation of repressive measures under the guise of cyber security can erode public trust. This erosion may lead to decreased cooperation between citizens and authorities, which is crucial for effective cyber security.

Building Human Capital: Establishing specialized training programs for cyber security professionals are necessary to address the skills gap.

Promoting Public Awareness: Launching nationwide campaigns to educate citizens about cyber security hygiene can reduce vulnerabilities.

Fostering Public-Private Partnerships: Collaborating with private sector stakeholders can leverage expertise and resources for a holistic cyber security strategy.

Developing a Comprehensive National Cyber Security Strategy: Drafting and implementing a national strategy addressing governance, incident response, and data protection is imperative.

Securing Critical Sectors: Mandating cyber security compliance for financial institutions and government agencies can safeguard critical infrastructure.

Establishing International Collaboration: Partnering with global cyber security organizations to adopt best practices and share intelligence is beneficial.

CONCLUSION

In conclusion, cyber security governance in Bangladesh, as outlined under the Cyber Laws, particularly the ICT Act 2006 and the Cyber Security Act 2023**,** establishes a robust legal framework for addressing the growing concerns related to digital security. The enactment of these laws has introduced various mechanisms, including the establishment of agencies, tribunals, and councils, to ensure effective governance and response to cyber threats. Key bodies such as the National Cyber Security Agency and the Cyber Security Council play pivotal roles in formulating national strategies, overseeing compliance, and coordinating efforts across sectors. While significant strides have been made in improving cyber security governance, continuous adaptation to emerging threats, enhanced coordination among stakeholders, and the development of a skilled workforce remain crucial for creating a secure digital environment in Bangladesh. Furthermore, strengthening Bangladesh's cyber security governance requires a multi-faceted approach. First, it is essential to implement comprehensive laws that balance state interests with individual rights to ensure a robust legal and regulatory framework. Investing in advanced cyber security technologies for threat detection and mitigation, along with building human capital through specialized training programs, is crucial to addressing the growing skills gap. Promoting public awareness through nationwide campaigns will help citizens understand cyber security hygiene, reducing vulnerabilities. Additionally, fostering public-private partnerships can enhance resource sharing and expertise. A comprehensive national cyber security strategy that includes incident response, data protection, and governance is necessary to guide the country's efforts. Ensuring that critical sectors, including financial institutions and government agencies, comply with cyber security standards will protect national infrastructure. Finally, international collaboration will allow Bangladesh to adopt global best practices and share intelligence, strengthening the country's cyber security resilience.

REFERENCES

1. Aguilera, R. V., Desender, K. A., Bednar, M. K., & Lee, J. H. (2020). Cybersecurity governance: A path to building trust in an organization. MDPI Future Internet, 12(3), Article 54. DOI: 10.3390/fi12030054.
2. Ahmed, R. (2022). Data Protection Laws and Their Impact on Cybersecurity in Bangladesh. International Journal of Cyber Law, 8(1), 22-35.
3. Ahmed, S., & Rahman, M. (2023). The Evolution of Cyber Security Laws in Bangladesh: An Analysis of the Cyber Security Act 2023. Journal of Digital Policy and Governance, 12(3), 45-62.
4. Alotaibi, S., & Almagwashi, H. (2021). A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy, 3(3), 17.

5. Amnesty International (2024, August 8). Bangladesh: Interim Government must restore freedom of expression in Bangladesh and repeal Cyber Security Act. News. Available at: https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/?utm_source=chatgpt.com.
6. Anmar Frangoul (2018, February 9). 10 ways the web and internet have transformed our lives. CNBC. Available at: https://www.cnbc.com/2018/02/09/10-ways-the-web-and-internet-have-transformed-our-lives.html.
7. Badruzzaman, M. (2016). Controversial Issues of Section-57 of the ICT Act, 2006: A Critical Analysis and Evaluation. IOSR Journal of Humanities and Social Science, 21(1), 62-71.
8. Bangladesh Information Communication Technology Act 2006, November 2023.
9. Bashar, A. (2023). Cyber Security Governance in Bangladesh: A Legal Overview. Bangladesh Journal of Cyber Law, 12(2), 45-60; Rahman, M. & Khan, S. (2023). Cyber Security and Legal Frameworks in Bangladesh: A Critical Analysis of the Cyber Security Act 2023. South Asian Journal of Law and Technology, 7(1), 30-50.
10. BTRC. Number of Internet Subscribers. Available at: http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-july-2020.
11. Chowdhury, S., & Rahman, M. (2021). Public Key Infrastructure and Cybersecurity Governance in Bangladesh: The Role of the ICT Act, 2006. Journal of Digital Security Studies, 8(4), 113–125. DOI: 10.1080/jdss.2021.009887.
12. Cyber Security Capacity Review Bangladesh, 2018. NRD Cyber Security, Global Cyber Security Capacity Center, Oxford Martin School, Oxford University, p.48. Available at: https://www.nrdcs.lt/file/repository/resources/CMM_Bangladesh_Report_FINAL.pdf.
13. Dhaka Tribune Desk (2023, September 20). Editors' Council concerned over passing of Cyber Security Act-2023. Dhaka Tribune. Available at: https://www.dhakatribune.com/bangladesh/325860/editors%E2%80%99-council-concern-over-passing-of-cyber?utm_source=chatgpt.com.
14. International Commission of Jurists (November 2013).
15. Khan, T., & Alam, R. (2023). Balancing Security and Freedom: The Challenges of Implementing the Cyber Security Act 2023 in Bangladesh. Bangladesh Law Review, 9(2), 112-129.
16. Korea International Cooperation Agency (2018). E-Government Master Plan for Digital Bangladesh. Available at: http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd.
17. Kumar, P., & Lee, J. (2023). Innovative Network Security Approaches for Hybrid Work Environments. Journal of Network Security Research, 18(1), 54-69.
18. Mamun, Abdullah Al, Jamaludin Bin & Sk. Mamun Mostofa (2021). Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies.
19. Masum Billah & Aunim Shams (2023, July 8). Sound the alarm bell: Inside the leak of 50 million Bangladeshis' personal data. Available at: https://www.tbsnews.net/bangladesh/inside-leak-50-million-bangladeshis-personal-data-662174.
20. Mohammad Nur Nabi, Muhammad Tanjimul Islam (2014, October). Cyber Security in the Globalized World: Challenges for Bangladesh. Conference: Economic and Social Development, 7th International Scientific Conference, New York, USA.
21. National Cybersecurity Strategy of Bangladesh, 2014. Available at: http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf.
22. NCSI. Bangladesh. Available at: https://ncsi.ega.ee/country/bd/.
23. Nguyen, L., & Harris, K. (2021). The Impact of Security Awareness Training on Employee Behavior. Journal of Information Security Education, 9(4), 87-101.
24. Pushpo, F. H., & Uddin, M. K. (2022). Adoption of International Management Standards in Bangladesh: Progress and Prospect. Proceedings of the 5th International Conference on Industrial & Mechanical Engineering and Operations Management (IMEOM), Dhaka, Bangladesh, December 26-27, 2022.
25. Rahman, M., & Khan, S. (2023). Cyber Security and Legal Frameworks in Bangladesh. Journal of Cyber Security and Law, 12(3), 47-68.
26. Rodriguez, C., & Patel, V. (2023). Optimizing Incident Response Strategies in Evolving Threat Landscapes. Cybersecurity and Resilience Journal, 15(2), 112-125.

27. Sarker, Sree Pradip Kumer, & Raza Zahir Khan (2024). Cybersecurity Considerations for Smart Bangladesh: Challenges and Solutions. Asian Journal of Research in Computer Science, 17(6), 145-156. DOI: 10.9734/ajrcos/2024/v17i6464.
28. Shahriar Rumi (2025, January 30). HIPAA and Healthcare IT Security: A Critical Need for Bangladesh.
29. Simon Kemp (2018). Digital in 2018: World's Internet Users Pass the 4 Billion Mark. Available at: https://wearesocial.com/blog/2018/01/global-digital-report-2018.
30. Smith, A., & Jones, B. (2022). Enhancing Cyber Risk Management Frameworks for Modern Enterprises. Journal of Cyber Risk, 10(3), 215-230.
31. Syed Shadman Wahid (2024, May 12). Cybersecurity in Critical Information Infrastructure of Bangladesh, The Financial Express.
32. Transparency International Bangladesh, Cyber Protection Ordinance 2024:TIB Warns of Risks to Media Freedom, Organizational Rights, and Freedom of Expression, See at:https://www.ti-bangladesh.org/articles/press-release/7175?utm_source=chatgpt.com
33. Uddin, M. R. (2021). The National Cybersecurity Strategy of Bangladesh: A Critical Analysis. Cybersecurity and Cyber Diplomacy at the Crossroad: An Appraisal of Evolving International Legal Developments in Bangladesh Context. Retrieved from