ARTICLE 19
Defending freedom of expression and information

TRANSPARENCY INTERNATIONAL BANGLADESH
Social movement against corruption

Review of Proposed Cyber Security Rules, 2024

Quazi MH Supan
Associate Professor
Department of Law
University of Dhaka
Email: qmhsupan@du.ac.bd

13 June 2024

Abbreviations

AI	Artificial Intelligence
CERT	Cyber Emergency Response Team
CII	Critical Information Infrastructure
CIRT	Computer Incident Response Team
CSA	Cyber Security Act, 2023
DB	Detective Branch
DFL	Digital Forensic Lab
DGFI	Directorate General of Forces Intelligence
IoT	Internet of Things
NCERT	National Cyber Emergency Response Team
NCSA	National Cyber Security Agency
NSI	National Security Intelligence
OS	Operating System
PBI	Police Bureau of Investigation
PDA	Personal Digital Assistance
RAB	Rapid Action Battalion
RAM	Random Access Memory
SB	Special Branch

Review of Proposed Cyber Security Rules, 2024

Background

Realizing that a 'dependable information system is essential for efficient management and operation of the public and private sectors'[1] and also comprehending that 'there is a shortage of locally generated information needed for efficient performance of these sectors'[2], Bangladesh settled her goal to accelerate ICT use in every sector in terms of information generation, utilization and applications. As Bangladesh intends to use ICT as the key-driving element for socio-economic development, Bangladesh published her first ever National Information and Communication Technology (hereinafter referred to as ICT) Policy in October, 2002 to be regarded as national ICT strategy as a part of the overall national development plan[3]. The ***Vision and Objectives*** segment of the Policy states:

> ... a country-wide ICT-infrastructure will be developed to ensure access to information by every citizen to facilitate empowerment of people and enhance democratic values and norms for sustainable economic development by using the infrastructure for human resources development, governance, e-commerce, banking, public utility services and all sorts of on-line ICT-enabled services[4].

The 2002 ICT Policy understood the importance of establishing legislative and regulatory framework for data security and protection[5], and thus, felt the necessity for immediate enactment of an ICT Act to protect against computer crimes such as computer fraud, hacking and damage to programs and data and introducing/spreading computer viruses[6]. To ensure data security and interoperability and freedom of information, the 2002 ICT policy emphasized on setting of encryption standards and international agreements on interoperability[7] and formulation of new laws or amendment to the existing ones[8].

The first ever cyber law in its true sense was enacted in 2006. The Information and Communication Technology Act, 2006[9] was enacted to 'make rules to provide legal recognition and security of Information and Communication technology and other relevant matters.'[10] The law, among others, criminalizes certain cyber activities and makes provisions for Cyber Tribunal and Cyber Appellate Tribunal. The law failed to deliver its preambular objective and raised huge controversy specially for its vague definition of crime that was abused to criminalize freedom of expression.

---

1 Ministry of Science and Information & Communication Technology, Government of the People's Republic of Bangladesh, 'National Information and Communication Technology (ICT) Policy' (October 2002) < https://www.rhd.gov.bd/Documents/MISandEstates/National%20ICT%20Policy/NationalICTPolicy.pdf> accessed 15 April, 2024, Preambular paragraph 1.2.

2 Ibid.

3 Ibid., paragraph 1.3.

4 Ibid., paragraph 2.1.

5 Ibid., paragraph 2.2.5.

6 Ibid., paragraph 3.7.2.

7 Ibid., paragraph 3.7.3.

8 Ibid., paragraph 3.7.4.

9 Act No, 39 of 2006 (http://bdlaws.minlaw.gov.bd/act-details-950.html)

10 Preamble, the Information and Communication Technology Act, 2006.

To ensure cyber security, the 2009 ICT Policy proposed introduction of cyber police[11] and Establishment of special tribunal(s) to prevent cybercrimes and IPR crimes[12].

Under the Information and Communication Technology Act, 2006, the first ever Cyber Tribunal was established in Dhaka 2013[13]. Later, on 4 April 2021, seven more Cyber Tribunals were established[14] and thus, total number of Cyber Tribunals now stands at 8.

Serial	Name of the Tribunal	Local Jurisdictional Area
1	Cyber Tribunal, Dhaka	Dhaka, Narsingdi, Gazipur, Shariatpur, Narayanganj, Tangail, Kishoreganj, Manikganj, Munshiganj, Rajbari, Madaripur, Faridpur and Gopalganj
2	Cyber Tribunal, Chittagong	Chittagong, Comilla, Brahmanbaria, Chandpur, Lakshmipur, Noakhali, Feni, Cox's Bazar, Bandarban, Rangamati and Khagrachhari
3	Cyber Tribunal, Rajshahi	Rajshahi, Sirajganj, Pabna, Bogura, Natore, Joypurhat, Chapai Nawabganj and Naogaon
4	Cyber Tribunal, Khulna	Khulna, Jashore, Bagerhat, Satkhira, Meherpur, Narail, Chuadanga, Kushtia, Magura and Jhenaidah
5	Cyber Tribunal, Barisal	Barisal, Jhalokati, Patuakhali, Pirojpur, Barguna and Bhola
6	Cyber Tribunal, Sylhet	Sylhet, Moulvibazar, Habiganj and Sunamganj
7	Cyber Tribunal, Rangpur	Rangpur, Dinajpur, Kurigram, Nilphamari, Lalmonirhat, Gaibandha, Thakurgaon and Panchagarh
8	Cyber Tribunal, Mymensingh	Mymensingh, Sherpur, Jamalpur and Netrokona

The 2015 ICT Policy added more issues to 'To Do' list to ensure cyber security. They include:

- Establish special unit for police to investigate cybercrimes;[15]
- Constitute Computer Emergency Response Team; [16]
- Establish Cyber Security Agency under the ICT Department; [17]
- Establish Special Tribunal to control cybercrimes and IPR crimes;[18]
- Enact new law and amend existing laws to secure electronic transactions.[19]

Among all the ICT Polices, the Policy of 2018 put the highest emphasis on cyber security. Among the objectives of the Policy, digital security was the second one and it aspired to make

11 ICT Policy 2009, serial 275 at page 49.
12 Ibid., serial 277 at page 49.
13 SRO No. 27-Law/2013 dated 28 January, 2013.
14 SRO No. 83-Law/2021 dated 4 April, 2021.
15 Serial 159, Bangladesh Gazette, Extraordinary, August 5, 2015, page 6307.
16 Serial 160, Bangladesh Gazette, Extraordinary, August 5, 2015, page 6307.
17 Ibid.
18 Serial 161, Bangladesh Gazette, Extraordinary, August 5, 2015, page 6308.
19 Serial 164, Bangladesh Gazette, Extraordinary, August 5, 2015, page 6308.

the use of information and communication technology safe and risk-free in all spheres.[20] Its strategic objectives wanted to:[21]

- Encourage use of quality hardware/software in digital devices to ensure digital security;
- Ensure safe use of Internet;
- Take measures to protect confidentiality of private information;
- Take initiatives to protect women and children from harmful contents of all digital media including social media;
- Take appropriate steps to prevent digital crimes;
- Follow optimal rules and standards in information management and security;
- Ensure safe use of information technology in financial transactions;
- Ensure preservation of all digital transaction logs for forensic investigation.

Additionally, the policy included cypher security issues like increased cooperation among public and private organizations to prevent digital crimes;[22] preparation and implementation of national digital security framework;[23] establishment of digital security agency;[24] digital crisis management;[25] and enforcement of relevant laws to prevent cybercrimes.[26]

In the high tide of policy impetus, the Digital Security Act, 2018 was enacted amidst vehement opposition and criticism from the civil society and human rights organizations: national, regional and international. The first Digital Security Agency was established in December 5, 2018 under section 5 of the DSA. In 2023 the Government enacts the Cyber Security Act, 2023 repealing and slightly modifying the DSA. In the same year the Government establishes the National Cyber Security Agency on 7 November. However, the Digital Security Agency failed to initiate its assigned role due to lack of equipment and manpower. As of December 2023, the Agency had about a dozen individuals and none of them were permanent staff members and most of them did not have any expertise in cybersecurity. And according to a Daily Star report[27] the 'agency has also become a revolving door of directors: it saw six directors leave this year [2023]'. In this scenario the Government has proposed new Cyber Security Rules, 2024.

Cyber Security Rules, 2024: Narrow Ambit

From the title of the rules (Cyber Security Rules, 2024), one would reasonably expect that these rules will be comprehensive in nature with wider perspectives and issues dealt with in the parent law, i.e., the Cyber Security Act, 2023. However, a close examination of the said rules reveals a very narrow scenario. It deals with the following issues:

Rules	Dealing with
Rules 3-7	Manpower, powers, responsibilities, functions of the National Cyber Security Agency (NCSA)

[20] Bangladesh Gazette, Extraordinary, December 15, 2018, page 26070.
[21] Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26071-2.
[22] Serial 2.5.4, Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26092.
[23] Serial 2.5.6, Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26093.
[24] Serial 2.5.7, Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26093.
[25] Serial 2.5.8, Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26093.
[26] Serial 2.5.9, Bangladesh Gazette, Extraordinary, December 15, 2018, pages 26093.
[27] Cyber Security Agency exists only in name, The Daily Star, 30 November 2023 (https://www.thedailystar.net/news/bangladesh/news/cyber-security-agency-exists-only-name-3482396)

Rules 8-13	Responsibilities and functions of the National Computer Emergency Response Team (NCERT)
Rules 21-24, Scedule-2	Digital Forensic Lab (DFL)
Rule 16-17, Schedule-1	Critical Information Infrastructure

A plethora of critical issues that could be dealt with by these rules are missing from it. For example:

- Required qualifications of the National Cyber Security Agency[28], National Computer Emergency Response Team (NCERT) and Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT)[29] or and digital forensic lab (DFL) personnel[30];
- What legal, diplomatic and procedural methods the National Cyber Security Agency, National Computer Emergency Response Team (NCERT) and Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT) will follow for cooperation and exchanging information with foreign agencies and organizations[31].
- How the NCSA will coordinate among NCERT, CERT and CIRT and supervise them[32].
- Critical Information Infrastructure[33] criteria not set[34].
- Qualifications of CII audit and inspection personnel not set[35].
- The provisions of the CSA[36] that arguably criminalizes freedom of expression by way of restricting and compromising freedom of speech, dissent, thought and conscience, freedom of the press and investigative journalism could be soften and flexed by incorporating explanations and territorially binding the offenders to the local jurisdictions to avoid multiplicity of proceedings. Explanations could also be used to remove the vagueness in various offence definitions to prevent potential misuse.
- As digital evidence is fundamentally different from other types of evidence and can easily be altered, the Rules could offer a new Search List instead of old B.P. Form No. 44 (Bengal Form No. 5276). Under the current scenario the prosecution will find it extremely difficult to prove the authenticity of digital evidence acquired by the investigation officers under Sections 40. (1), 41. (a) (i) and 42. (1) (b).
- Perhaps the most important issue the Rules missed out is regional and international cooperation regarding investigation and prosecution of cybercrimes. Section 54 of the parent law emphasizes on the application of the Mutual Legal Assistance in Criminal Matters Act, 2012. The Mutual Legal Assistance Treaty (MLAT) process facilitates the production of digital evidence in cross-border investigations when the crime occurs in one country but data is held by a company in another country. Kent Walker, the President of Global Affairs at Google and Alphabet, writes:

> Without better and faster ways to collect cross-border evidence, countries will be tempted to take unilateral actions to deal with a fundamentally multilateral problem. A sustainable framework for handling digital evidence in legitimate

[28] Sections 6. (1) and 7. (2), the Cyber Security Act, 2023.
[29] Ibid., Section 9. (3).
[30] Ibid., Section 11. (2) (a).
[31] Ibid., Section 9. (5) (d).
[32] Ibid., Section 9. (6).
[33] Most countries have enacted laws that provides criteria for CIIs. See for example, Czech Republic criteria: https://nukib.gov.cz/download/publications_en/support_materials/KII_rozhodovaci_schema_EN_final.pdf.
[34] Ibid., Section 15.
[35] Ibid., Section 16. (4).
[36] Ibid., Sections 21, 25, 26, 28, 29 and 31.

> cross-border investigations will help avoid a chaotic, conflicting patchwork of data location proposals and *ad hoc* surveillance measures that may threaten privacy and generate uncertainty, without fundamentally advancing legitimate law enforcement and national security interests.[37]

This is particularly true for Bangladesh as studies show major cyber-attacks on Bangladeshi Government and private websites originate abroad[38]. Without effective use of MLAT prosecution of cyber criminals will be futile due to lack of evidence. The current Rules could incorporate elaborate provisions for initiating and executing MLATs. The Rules could take the opportunity to make provisions for MLAT funding, issue unilateral guidelines for direct data requests, streamline the MLAT process, adopt industry-wide legal interpretations for data requests and renegotiate existing MLATs[39].

Digital Security Rules, 2020 Vs Cyber Security Rules, 2024

In most part, the Cyber Security Rules, 2024 is a verbatim reproduction of the Digital Security Rules, 2020. Out of 26 Rules, 19 rules have been borrowed verbatim from the Digital Security Rules, 2020.

Provisions	Digital Security Rules, 2020[40]	Cyber Security Rules, 2024[41]	Difference
Definition	Rule 2	Rule 2	Verbatim
Powers of the Digital/National Cyber Security Agency	Rule 3	Rule 4	Verbatim
Manpower of the National Cyber Security Agency	-	Rule 3	New addition
Responsibilities and Functions of the Digital/National Cyber Security Agency	Rule 4	Rule 5	Verbatim
Powers and Responsibilities of the Director General	Rule 5	Rule 6	Verbatim
Powers and Responsibilities of the Directors	-	Rule 7	New addition
Responsibilities and functions of the National Computer Emergency Response Team	Rule 6	Rule 8	Verbatim
Providing information relating to digital/cyber security, etc.	Rule 7	Rule 9	Verbatim
Office of the National Computer Emergency Response Team	Rule 8	Rule 10	Verbatim

[37] Kent Walker, An International Framework for Digital Evidence, blog.google, 2017. (https://blog.google/outreach-initiatives/public-policy/international-framework-digital-evidence/#:~:text=The%20Mutual%20Legal%20Assistance %20Treaty,a%20company%20in%20another%20country).).

[38] Bangladesh Cyber Threat Landscape 2022, Cyber TIIR, BGD e-GOV CIRT, 2022. (https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf).

[39] For various perspectives on the issue, see Jonah Force Hill, Problematic Alternatives: MLAT Reform for the Digital Age in National Security Journal, Harvard Law School, Online Edition, January 2015. (https://harvardnsj.org/2015/01/28/problematic-alternatives-mlat-reform-for-the-digital-age/).

[40] Made in exercise of power conferred by Section 60 of now repealed [repealed by Section 59. (1) of the Cyber Security Act, 2023 (Act No. 39 of 2023)] the Digital Security Act, 2018 (Act No. 46 of 2018).

[41] Proposed to be made in exercise of power conferred by Section 58 of the Cyber Security Act, 2023.

Fulltime responsibilities of the National Computer Emergency Response Team	Rule 9	Rule 11	Verbatim
Exchange of information	Rule 10	Rule 12	Verbatim
Taking measures in response to incidents relating to digital/cyber security	Rule 11	Rule 13	Verbatim
Identification of Critical Information Infrastructure	Rule 19	Rule 14	Verbatim
Evaluation of Critical Information Infrastructure	Rule 12	Rule 15	Verbatim
Establishment of Digital Forensic Lab	Rule 13	Rule 21	Verbatim
Standards to be followed by the Digital Forensic Lab	Rule 14	Rule 22	Verbatim
Forensic analysis of evidence	Rule 15	Rule 23	Verbatim
Manpower of digital forensic lab	Rule 16	Rule 24	Verbatim
Essentials to be followed by individuals or organizations running Critical Information Infrastructure	Rule 17	Rule 16	Verbatim
Audit of Critical information infrastructure	Rule 18	Rule 17	Verbatim
Critical information infrastructure Audit Mandate	-	Rule 18	New addition
Formulation of Audit Panel by the National Cyber Security Agency	-	Rule 19	New addition
Qualification for inclusion in the Audi Panel	-	Rule 20	New addition
Convening National Cyber Security Council meeting	-	Rule 25	New addition
Seeking assistance from relevant individual or organization	Rule 20	Rule 26	Verbatim
Rules and Procedures of IT Audit	-	Schedule-1	New addition
Digital Forensic Examination Procedures	Schedule	Schedule -2	Verbatim

National Cyber Security Agency (NCSA): Top-heavy Organization without any meaningful Organizational Structure

Under the parent law the NCSA should consist 1 Director General and a number of Directors specified by rules made thereunder. (Section 5.(1))

Rule 3.(1) of the Cyber Security Rules 2024 have proposed for five Directors, namely:

(a) Director (Administration and Finance)
(b) Director (Planning and Development)
(c) Director (Law and Coordination)
(d) Director (Operation - 1)
(e) Director (Operation - 2)

Accordingly, the NCSA will have six directors and thus, it may well become a top-heavy organization likely having a disproportionate number of higher-level employees in comparison to the number of front-line or lower-level employees. This can lead to a situation where multiple layers of management may slow down decision-making processes and communication flow within the agency. Additionally, it can create a situation where the agency will consume higher amount of tax-payers money due to the larger number of managerial positions. Operational inefficiency, bureaucratic bottlenecks and reduced productivity are obvious outcomes of a top-heavy organization. Furthermore, Agency employee morale and engagement

may decline due to limited empowerment and a lack of avenues for collaboration and innovation.

NCSA's Obscure Organizational Structure

Almost all the national cyber security agencies currently working in different states employ a whole-of-government approach to investigate, disrupt and deter cybercrimes.[42] They work with other law enforcement agencies; the intelligence community; civil, administrative and regulatory agencies, prosecutorial service; and the military to draw upon each partner's unique expertise and resources, and to use whichever combination of tools will be most effective in responding to and countering a particular threat.[43]

The proposed Rules, taken together with its parent law, does not give us any clear organization structure as to its functioning. The Rules loosely and superficially elaborate the powers, functions and responsibilities of the NCSA, its Directors and NCERT. It fails to deliver NCSA's functionality structure at a larger landscape.

Firstly, other than the Director General and the Directors, it does not tell us anything about NCSA's internal organization structure and functionality; and secondly, it is silent on how it will interact other law enforcing agencies (SB, DB, PBI, RAB, Counter Terrorism, etc.), civil and military intelligence (NSI, DGFI), civil administration and prosecutorial service. The proposed Rules seems to be an attempt to establish NCSA as an isolated and independent organization. The present trend all over the world shows us such organizations cannot, should not and do not stand alone in isolation. Some NCSAs have good organization structures without any legislative intervention.

Qualifications of the Cyber Security Personnel Not Set

Personnel	Qualifications under the Cyber Security Act, 2023	Qualifications under the Proposed Cyber Security Rules
DG and Directors of the NCSA [44]	The Director General and the Directors shall be appointed by the Government from among persons having expertise in computer or cyber security and the terms and conditions of their service shall be determined by the Government.	Silent
NCERT[45]	The Computer Emergency Response Team and Computer Emergency Team or Computer Incident Response Team shall consist of persons having expertise in cyber security and, if necessary, members of law enforcing agencies.	Silent
NCSA Employees[46]	Terms and conditions of service of Agency employees shall be determined by Rules.	Silent
DFL Personnel[47]	Personnel with appropriate qualifications and training	Personnel with appropriate

42 See, Annexes 1-3.

43 David H. Laufman et al, Cyber incidents: How best to work with law enforcement in Cyber Security: A Peer-Reviewed Journal Vol. 1, 2 102–115, Henry Stewart Publications 2398-5100 (2017).

44 The Cyber Security Act, 2023, Section 6. (1).

45 Ibid., Section 9.

46 Ibid. Section 7. (2).

47 Ibid., Section 11. (2) (a).

		qualifications and training[48]
CII security auditors and inspectors[49]	Persons having expertise in cyber security	Qualifications determined by the Agency[50]

Under the current legal framework , the qualifications required to be cyber security personnel remain vague as what constitutes 'expertise in computing and cyber security' is undeterminable without any fixed set of standards. The proposed rules have failed disastrously to set such standards. This is alarming because most of the Digital Security Agency, the predecessor of the NCSA, did not have any expertise in cyber security[51]. The proposed Rules could detail on qualifications of various personnel employed by the CSA and there are some recognized cyber security personal traits and government and private cyber security agencies all over the world look for personnel having such traits.

Cybersecurity skills are the qualifications and capabilities required to work effectively and meaningfully in a cyber security organization and when such organization is national one such qualifications are *sine qua non*. Cybersecurity experts work within an organization to keep data, networks and systems safe and secure. They monitor current systems for both internal and external threats and risks posed by any outside services the company accesses and uses. They also assess risk, troubleshoot problems and create solutions for optimal system security. As complex technologies continue to evolve, cybersecurity experts are continually developing new skills to help them prevent and combat cyberthreats to individuals and businesses and government cyber resources.

There are some essential cyber security skills the cyber security personnel rely on to actually get their work done, collaborate with others, and accomplish their professional goals. As public and private activities are become increasingly reliant on cyber technology, the need for qualified cyber security professionals continues to grow. In order to stay ahead of the latest cyber threats and security breaches, it's important to have Agency personnel with these top cybersecurity traits in place[52].

Skill	**Explanation**
Critical thinking skills	In order to keep up with the latest cybersecurity threats, a robust cyber security agency needs staff members who can analyze data, identify vulnerabilities, and come up with creative solutions. Cybersecurity is all about solving complex problems and spotting security vulnerabilities. Individuals who are able to think critically and come up with creative solutions are essential in this field. Critical thinking skills can help Agency members, among others, to:

48 The Proposed Cyber Security Rules, 2024, Rule 22. (2) (a).
49 Ibid., Section 16. (4).
50 The Proposed Cyber Security Rules, 2024, Rule 19. (1)
51 Cyber Security Agency exists only in name, The Daily Star, 30 November 2023 (https://www.thedailystar.net/news/bangladesh/news/cyber-security-agency-exists-only-name-3482396)
52 Anne-Marie Mohammed (The University of the West Indies, St. Augustine, Trinidad and Tobago), Vladlena Benson (Aston Business School, UK), and George Saridakis (University of Kent, UK), Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites in Mehdi Khosrow-Pour, D.B.A. (ed.), Encyclopedia of Criminal Activities and the Deep Web, IGI Global, 2020.

	• Ask the right questions • Evaluate and assess data • Identify your assumptions • Consider alternatives • Understand context • Draw data-driven conclusions
Strong Communication Skills	Many times, cyber security personnel are responsible for explaining technical information to non-technical staff or management. In order to be successful in this field, they need to be able to communicate effectively and understand the needs of their audience. Cybersecurity is a complex field, and without good communication skills, a lesser cybersecurity specialist may struggle to be effective in their role. Both written and verbal communication play a key role in cybersecurity. A member of the staff may need to communicate technical concepts to individuals without a technical background, such as executives or legal teams. They may also be asked to write incident reports, where they will have to document what they did in a concise and clear manner.
Collaboration	A cybersecurity expert will likely work with a larger security team of other cybersecurity professionals. S\he may also need to collaborate with other legal, IT, public relations teams within the Agency or share findings with other organizations or the greater cybersecurity community.
Risk management	Cyber security experts must have the ability to think through what could possibly go wrong, assess the severity of threats, and gauge the potential impacts on cyber resources.
Problem-solving skills to resolve security issues quickly	Cybersecurity isn't just about knowing how to use antivirus software or firewalls. It's also about being able to identify and solve problems quickly and efficiently as these professionals will be working as part of a team where their job is to analyze data and identify potential issues before they escalate into larger problems. From working directly with national and private organization leaders and IT teams to identify potential risks to helping them develop effective countermeasures, being able to quickly understand complex information and translate it into actionable steps is key. Ultimately, the best cybersecurity professionals know how to solve problems and aren't afraid to dive headfirst into complex projects and figure things out as they go along.
Technical skills in the latest cybersecurity technologies	While having strong critical thinking and problem-solving skills is key, cyber security experts also need to be well-versed in the latest technologies used in today's digital landscape. The cybersecurity field is constantly evolving, and they need to be able to keep up with the latest trends and technologies. What this means is that they should have a strong understanding of network security, malware analysis, cryptography, artificial intelligence, etc.
High ethical standards to avoid internal cybersecurity risks	One issue that often comes up during the recruitment process is ethics. In order for an Agency to trust its cybersecurity infrastructure to someone, they need to know that this person upholds high ethical standards both in their professional and personal life. After all, the last thing a national cyber security organization wants is someone compromising organization's security by taking shortcuts or engaging in unethical behavior.
Legal knowledge	Types of digital forensics deal with discovering and preserving evidence that can be used in court. Those who are involved in this field need to have a solid understanding of the laws and regulations that pertain to data protection.
Human Rights Knowledge	While investigating a case, digital forensic practitioners can come across sensitive data, without getting a proper warrant, which violates the individual's right to privacy. There is also potential for bias and discrimination, while collecting and analyzing evidence. Knowingly or unknowingly digital forensic tools can be used in violation of individuals' right to privacy and confidentiality of communication,

	right to fair trial, etc. It is essential that cyber security personnel possess a working knowledge of the human rights of the citizen.

Absence of Transparency and Accountability Mechanism

Neither the parent law nor the proposed rules offer any mechanism or reporting procedure to ensure transparency and accountability in the NCSA activities. There is no provision for independent oversight bodies to monitor the NCSA's activities and ensure compliance with human rights standards. A top-heavy NCSA with an unclear structure, coupled with government control, creates a high risk of Privacy violations, government surveillance and lack of accountability.

Narrow meaning of Critical Information Infrastructure

The definition of CII in Section 2. (1) (g) of the CSA is incomplete and does not follow any recognized methodology to identify a CII:

> "Critical Information Infrastructure" means any physical or virtual information infrastructure declared by the government which is capable of controlling, processing, circulating or preserving any information, data or electronic information and which if it is damaged or compromised may adversely affect
> (i) public safety or financial security or public health,
> (ii) national security or national integrity or sovereignty.

The Rules could provide an indicative list of critical sectors. For example:[53]

- Energy
- Information, Communication Technologies (ICT)
- Water
- Food
- Health
- Financial Services
- Public & Legal Order and Safety
- Civil Administration
- Civil Protection
- Transport
- Industry, specially, Chemical and Nuclear Industry
- Space and Research
- Environment
- Defence
- Intelligence

Indicative impact criteria to Identify CII[54]

Criteria	Explanation
Population affected	The percentage of the population affected from the disruption of the service
Concentration	The density of the population on the geographic area affecting the service

[53] European Union Agency for Network and Information Security, Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks, ENISA, December 2014.

[54] Ibid., pp 23-24.

Economic Impact	The cost of service disruption in terms of GDP percentage.
Public confidence	The effect that the proper operation of this service has on the public confidence towards the government
International Relations	The effect that that a service interruption will have on the relationships with other countries.
Public order	The effect that a service interruption may cause to the public order
Public operations hindered	The daily operations of the public, such as going to work via public transportation, are stopped or thwarted
3rd party foreign services are affected	Inter-dependencies with critical services of other country

Standards to be Followed by Digital Forensic Lab

The Rules have set certain standards to ensure quality of digital forensic procedures. Such standards are intended to ensure quality of services and systems that are safe, reliable, and consistent. ISO standards draw on international expertise and experience and are therefore a vital resource for governments when developing public policy. It is not uncommon for national governments to ISO standards to support public policy by referencing ISO standards in regulations. However, in a country like Bangladesh, such standards may be extremely difficult to achieve. For instance, lack of commitment from management, non-cooperation among employees, and poor understanding of quality management can be a big problem for the DFL. Financial Restrictions can be another obstacle when implementing the standards. Without sufficient financial resources, it may be difficult for the DFL to meet all standard requirements. This is particularly true for Bangladesh as the already established digital forensic lab in the CID is facing serious resource constraints – financial, technical and human. Lack of incentives can lead the DFL employees to be reluctant to adopt the standards due to the changes, as they may want to avoid the extra work involved with implementing the standards.

Though these standards are not made mandatory, still the Government should revisit the idea of incorporating them in the Rules. The Rules should place more emphasis on national and international legal standards of DFL procedures. Again, the standards should appear in a tabular form with their latest and updated editions in a language understandable by general public.

DFL Procedural Standards[55]

Standards	Utility
ISO/IEC/BDS 17025	It is useful for any organization that performs testing, sampling or calibration and wants reliable results. This includes all types of laboratories, whether they be owned and operated by government, industry or, in fact, any other organization.
ISO/IEC/BDS 15489	It establishes the fundamental concepts and principles for creating, capturing, and managing records. This standard applies to records in any format, structure, or technological environment, regardless of time. It covers important aspects such as records, record systems, metadata, policies, assigned responsibilities, monitoring, training, analysis of business context, identification of records requirements, records controls, and processes for creating, capturing, and managing records.
ISO/IEC/BDS 27037	It provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

[55] For details, visit: https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0

ISO/IEC/BDS 27041	It provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process.
ISO/IEC/BDS 27042	It provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.
ISO/IEC/BDS 27043	It provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation.
ISO/IEC/BDS 27050	It provides an overview of electronic discovery. In addition, it defines related terms and describes the concepts, including, but not limited to, identification, preservation, collection, processing, review, analysis, and production of ESI.

Source Money and Risk Allowance

Rule 3. (2) introduces something not mentioned in the parent Act. In the name of state security, it entitles the NCSA to receive source money in special needs and it also entitles all the officers and employees of the NCSA to receive risk allowance. This should be essentially a legislative function as it is a very important policy content that should be a matter for Parliament to determine in the Act through an open democratic process. Still, the Rules could provide criteria for determining risk allowance. For example:

- The employment categories and payment of the risk allowance to employees attached to those employment categories having regard to the nature of their duties and the work environment;
- the nature and extent of the risk to which they are exposed;
- the frequency of the risk, i.e. when do the employees experience a genuine risk to their life during the course of their employment;
- the safety and precautionary measures the Agency has implemented to mitigate the risks;
- if mitigating measures are in place, the degree to which the risk could be mitigated. If not mitigated or partially mitigated the reasons that the risk persists and the degree to which it continues to present a genuine life-threatening risk to the employee; and
- substantive motivation provided by the Agency where the risks cannot be mitigated through safety and precautionary measures.

Without such criteria the delegated legislative power may be considered too broad or uncontrolled and thus, undermines the transparency and legitimacy of the law.

One solution for all problems: Branches of digital forensics ignored

Schedule 2 seems to be detached from reality. It does not reflect the advancement and technological and procedural development in the methodologies followed in a digital forensic lab. Digital forensic examination methods are centered around devices and file forensic.

Cyber security agencies in countries like Bangladesh that have resource constraints are mostly limited by the public sector budget and such budget constraint may encourage the government to employ single functionality digital forensic lab instead of bidding and installing an integrated all-function digital forensic lab. However, in essence, equipping a complete and scientific digital forensics lab has gradually been a consensus for countries who are dedicated to their citizen's safety and happinesses. With industry-standard case assistance capability and reliability makes much more sense than those solutions with simply lower cost, since what a law enforcement agency sets up for is for higher safety of the country and trustworthy solution help to achieve the goal.

Limited Functionality Digital Forensic Lab Limitations

Firstly, a limited functionality forensic lab is inherently unable to handle complex cases. Types of digital evidence are on the rise and will continue to do so (common types of digital evidence include logs, video footage and images, archives, active data, metadata, residual data, volatile data, replicant data). Often, it may be necessary to analyze data from multiple sources or to recover data that is hidden or encrypted. Limited functionality digital forensic lab may not have the capability to handle such complex cases, which can result in incomplete investigations. However, an integrated digital forensic laboratory can provide a comprehensive approach that allows multiple tools to work together, resulting in increased efficiency and accuracy, and enabling forensic analysts to handle complex cases.

Additionally, a limited functionality digital forensic lab will face difficulty in collaboration. Not only that digital evidence has different types of format and source, but when it's time for the analysis and conclusion of an investigative case, the cross-comparison and cooperation between different digital evidence would also have a tremendous impact on the investigation collaboration. In some cases, forensic analysts may have to use multiple branches of digital forensics to analyze different aspects of a case, and the lack of collaboration and communication between these branches may lead to missed evidence and incomplete investigations. An integrated digital forensic laboratory enables multiple branches to work together seamlessly, enhancing collaboration and communication and resulting in more accurate and thorough investigations.

- An integrated digital forensic lab has many advantages:
- Specialized tools and software that might not be available in a DFL with restricted capability can be accessed through an integrated DFL. This makes it possible for forensic analysts to examine digital evidence in greater details, which results in more precise and exhaustive investigations. For instance, specialized hardware for imaging and analyzing hard discs and other storage devices, as well as software for examining network traffic and other kinds of data, might be found in an integrated digital forensic lab.
- An integrated digital forensic laboratory provides a comprehensive and efficient approach to digital forensics, enabling forensic analysts to handle complex cases that involve multiple sources of data and encryption.
- An integrated digital forensic laboratory provides increased efficiency and accuracy by allowing multiple forensic tools to work together seamlessly. This results in better data processing and analysis and enables forensic analysts to handle complex cases that involve multiple sources of data and encryption. An integrated lab can also streamline the entire digital forensics process, allowing for faster turnaround times and more effective use of resources.

- Moreover, by having all the necessary tools and resources in one place, analysts can avoid the need to transfer data between different devices, which can lead to errors and delays.
- provide a centralized location for all forensic activities, allowing for better management of resources and more effective collaboration between investigators. the collaborative nature of an integrated laboratory enhances communication and collaboration among forensic analysts, leading to more accurate and thorough investigations.
- Additionally,
- An integrated digital forensic laboratory can help law enforcement agencies comply with industry standards for digital forensics. These standards ensure that digital evidence is collected, analyzed, and presented in a way that is admissible in court.

Digital forensics contains discrete branches based on the different sources of forensic data. Some of the most popular branches of digital forensics include:

Computer forensics: Identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media. This branch combines computer science and legal forensics to gather digital evidence from computing devices. It deals with the examination and analysis of computer systems and storage media to gather and preserve evidence in support of a legal case. emails.

Disk Forensics: It is branch of computer forensics that deals with extracting data from storage media by searching active, modified, or deleted files.

Mobile device forensics: This field involves the forensic examination and recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, tablets GPS devices, and game consoles. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Database forensics: Examining and analyzing databases and their related metadata to uncover evidence of cybercrimes or data breaches. This branch of digital forensics deals with the forensic analysis of databases, such as those used by financial institutions or government agencies, to recover and preserve evidence.

Digital Image Forensics: Extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.

Digital Video/Audio Forensics: Collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.

Network forensics: This area of digital forensics focuses on the analysis of network traffic to identify and track cyberattacks, such as hacking attempts or data breaches. It monitors, captures, stores and analyzes data found in computer network traffic, including web browsing and communications between devices in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.

Wireless Forensics: It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.

File system forensics: Examining data found in files and folders stored on endpoint devices like desktops, laptops, mobile phones, and servers.

Memory forensics: Recovery of evidence from the RAM of a running computer, also called live acquisition. It analyzes digital data found in a device's random-access memory (RAM). It collects data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

Email Forensics: Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

Malware Forensics: This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Forensic Data Analysis: This field involves the use of advanced analytical techniques and tools to extract meaning from large, complex data sets. For example, a forensic data analyst might use data mining and visualization techniques to identify patterns and relationships in financial transaction data in a fraud case.

Current digital evidence rules (Amended Evidence Act, 1872): Two different Jurisprudence?

Bangladesh followed India in amending the Evidence Act, 1872. To admit digital evidence in judicial proceedings, India amended her Evidence Act of 1872 by the Information Technology Act, 2000 (Act 21 of 2000). Bangladesh followed India verbatim in 2023.[56] Indian case laws on digital evidence admissibility have persuasive value in Bangladeshi courts. For example, in ***Mrs. Khaleda Akhter vs. The State[57],*** the Apex Court observed:

> A video cassette is a document within the meaning of the Evidence Act and is accordingly admissible in document. The Supreme Courts both in India and Pakistan approved of a tape record being used in evidence and that the use of the evidence by tape recording in a proceeding before a court of law.

Again, in Rajon murder case[58], the HCD argues:

> Per contra learned Deputy Attorney General submits that now it is well settled that video record is very much admissible evidence in the eye of law. In support of that he referred 37 DLR Khaleda Akter Vs. State Page-275 where it is held that "A video cassette is a document within the meaning of the Evidence Act and is accordingly admissible in document. The Supreme Courts both in India and Pakistan approved of a tape record being used in evidence and that the use of the evidence by tape-recording in a proceeding before a court of law. The process of tape-recording records only sound, whereas a video cassette or video records both sound and pictures. If sound be recorded on a tape is admissible in evidence, we do not see any difference in principle why the record of sound and pictures should not be equally admissible in evidence."

---

56 See Annex 05.
57 (1985) 37 DLR 275.
58 Death Reference No. 93 of 2015.

> In the above circumstances we do not find any logic in the argument of learned counsels for accused Kamrul, Moyan, Tazuddin and Zakir regarding the evidence of video footage. So we are also inclined to hold that a video record footage is a document within the incausing the Evidence Act and is accordingly admissible if otherwise relevant in causing of a trial of proceeding.

Various Laws of Bangladesh that Allow Digital Evidence in Legal Proceedings

Statutes	***Evidence***	***Sections***
STTA 2002	Audio, Video, Image	16
LODC (ST) A 2002	Audio, Video, Image	14
ICTA 2006	Electronic records-forms-gazettes-signatures-certificates, documents, data involved in EDI, data message (Email, SMS, etc.)	2, 6, 9, 10, 87
ATA, 2009	Facebook, Skype, Twitter Conversation, Offence related image or video	21(3)
PCA 2012	Electronic information, data Traffic data stored by BTRC, ISPs, MOs, VOIPSPs	6(2), 6(3)
MLACMA 2012	Computer data, traffic data stored by SPs	28-30
CSA 2023	Expert opinion, forensic evidence	56

Now, in India provisions of 65B. (4)[59] gave rise to conflicting interpretations. It states that if the electronic evidence is to be used in any judicial proceeding, a certificate shall have to be produced which identifies the electronic record, and gives particulars of the device involved in the production of the electronic record. This certificate shall have to be signed by a person occupying a responsible official position in relation to the operation of the relevant device, or from a person who is in the management of the relevant activities involved. This signature shall be evidence of the authenticity of the certificate. Section 65B(4) also mentions that the contents of the certificate should be stated "to the best of the knowledge and belief of the person stating it."

---

[59] Section 65B.(4):
In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, —
(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

The debate was concentrated on two issues: firstly, whether a certificate under Section 65B(4) must be produced even when an original record of the electronic evidence is available, or it has to be given only when a secondary record of the electronic evidence is produced; and secondly, whether compliance with Section 65B. (4) is mandatory even in a situation when it is not possible to obtain the certificate from the competent entity.

In ***State (NCT of Delhi) v. Navjot Sandhu***,[60] a submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution failed to produce the relevant certificate under section 65B. (4) of the Evidence Act, 1872. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.[61]

Anvar P.V. v. P.K. Basheer[62] dealt with the issue whether courts can admit electronic records as *prima facie* evidence without authentication. The Supreme Court declined to accept the admissibility of the electronic records as *prima facie* evidence without authentication in the court of law. It was held that in regard to any electronic record, for instance a CD, VCD, chip, etc., the same must be accompanied by the certificate according to the terms of section 65B obtained at the time of the taking the document, without which, the secondary evidence pertaining to that electronic record is inadmissible. Hence, strict compliance with section 65B is now mandatory for admissibility of the e-mails, web sites or any electronic record in a civil or criminal trial before the courts in India.

Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal and others,[63] the Court had to adjudicate on an election petition which challenged the election of Mr. Arjun Panditrao Khotkar from Jalna-101 Legislative Assembly Constituency on the ground that the nomination papers were filed after the stipulated deadline. The Respondents wished to rely on video camera recordings to prove that the candidate had filed his nomination after the stipulated deadline. The Election Commission produced CDs which contained a copy of the video camera recordings, in accordance with the direction given by the High Court. However, the necessary certificates were not produced in accordance with Section 65B. (4) by the Election Commission despite multiple requests made by the Petitioner.

During the cross examination, an officer of the Election Commission testified that the video camera recordings were authentic. Based on this testimony, the High Court admitted the evidence of the video recordings even though the certificate in accordance with Section 65B. (4) had not been produced. The High Court held that it was satisfied that there was "substantial compliance" with Section 65B, as a competent officer had testified that the video recordings were authentic.

---

60 (2005) 11 SCC 600, AIR 2005 SC 3820; 2005 Cri LJ 3950, 122 (2005) DLT 194(SC).

61 See also, Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178; Shahfi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801.

62 (2014) 10 SCC 473. Facts: Mr. P.V. Anwar filed an appeal, who had lost the previous Assembly election in Kerala, and contended that respondent Mr. Basheer was involved in tarnishing his image and his character by producing songs containing defamatory content on Compact Disk (CDs).

63 (2020) 7 SCC 1

Rakesh Kumar Singla v. Union of India[64] followed ***Arjun Panditrao Khotkar*** case. The learned counsel for the NCB placed reliance on WhatsApp messages by which the petitioner could be implicated. However, a certificate under Section 65B of the Indian Evidence Act was not available to authenticate the said messages. Therefore, the said message was held to be of no evidentiary value.

These rulings have serious implications for digital evidence admissibility in Bangladeshi courts. Although the amended Evidence Act of 1872 asks for authenticity certificate from the person(s) in managerial control of the data, the Cyber Security Act, 2023 and the proposed Cyber Security Rules, 2024 are silent on this very important issue. The recent studies show that major attacks on Bangladeshi CIIs originate abroad and prospective digital evidence remains in foreign jurisdictions, Moreover, cybercrimes committed using cloud and social media can be effectively prosecuted only when our law enforcing agencies will gain access to data stored in foreign jurisdiction. If we want to produce this data as digital evidence, under Evidence Act framework we also need certificates from those legitimate data holders in foreign jurisdictions. With the scarce use of MLAT that seems very improbable. The proposed Cyber Security Rules do not deal with this scenario. The DFL requires data to process and to acquire data we need a robust legal framework and proposed Rules fail to deliver that framework.

Furthermore, other than the amended Evidence Act of 1872, we have other statutes that allow us to introduce digital evidence in judicial proceedings and these 'other statutes' are mostly special laws. The Cyber Security Act, 2023 is also a special law[65]. These special laws pose a substantial risk of introducing a very different digital evidentiary jurisprudence other than the jurisprudence established by the Evidence Act, 1872 and the precedents.

Rule 26 *ultra vires* the Parent Law

Under special circumstances the Director General may seek assistance and advice from persons or organizations having expertise in cyber security and Rule 26 makes it mandatory for them to render their assistance and advice to the Director General. The parent law does not confer such power to the DG. The Rule goes beyond the parent law, the language used is harsh and may be regarded as giving arbitrary power to the DG. Such assistance should be made complimentary with or without incentives.

Misleading Use of Bangla

The language used in the proposed Rules is not easy reading and often unprofessional, inaccurate and misleading. For example:

Location	English	Bangla
Rule 13. (2) (h)	Denial of Service (DoS)	সেবা প্রদানে অস্বীকার করা
Rule 13. (2) (h)	Distributed Denial of Service (DDoS)	সেবা ও শ্রেণিকৃত সেবা প্রদানে অস্বীকার করা
Schedule-1	Fair presentation	ন্যায্যতা প্রদর্শন
Schedule-1	Due professional care	পেশাগত উৎকর্ষতা
Schedule-1	Independence	স্বাধীনতা

Conclusion

[64] CRM-M No. 23220 of 2020 (O&M)

[65] See, Section 3.

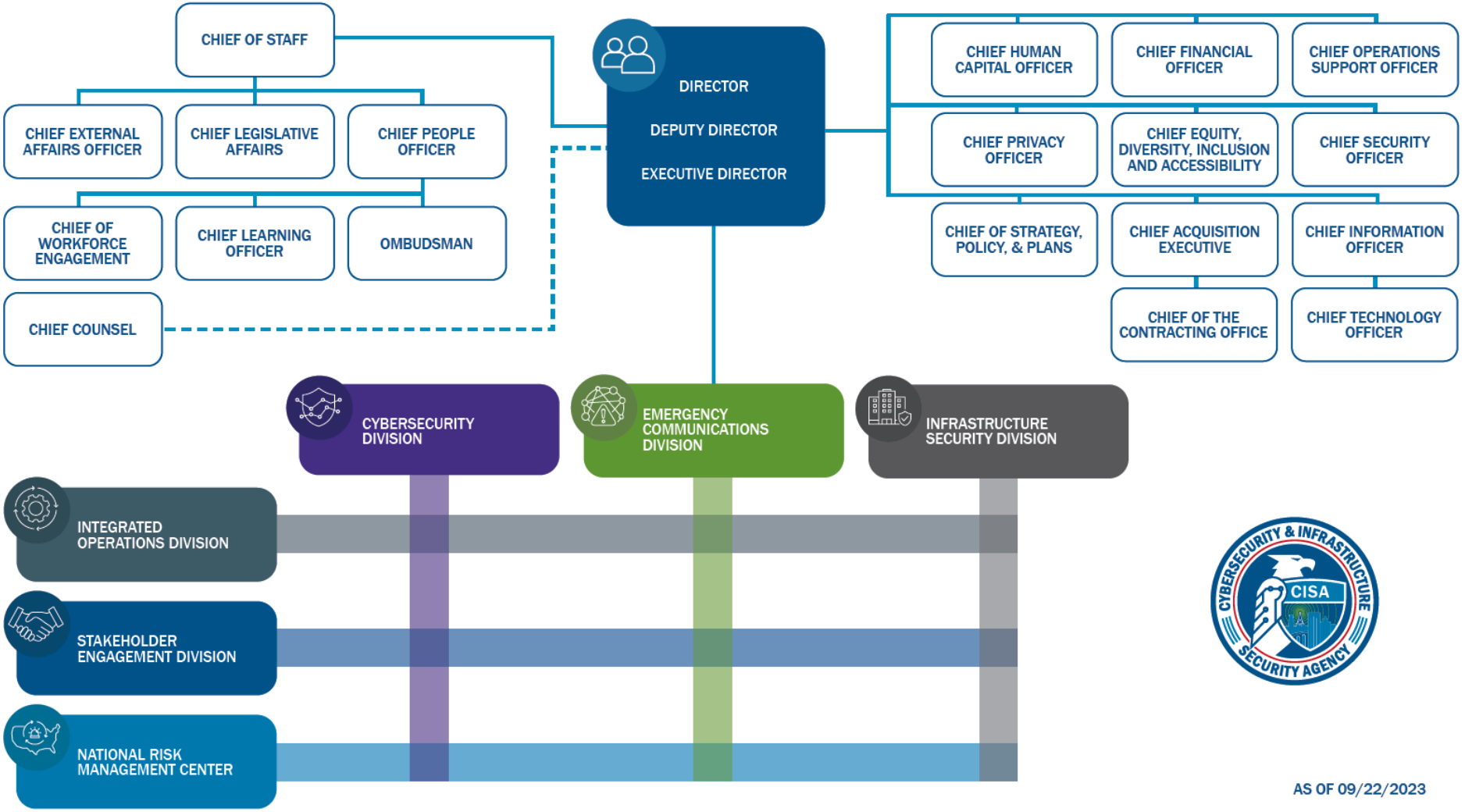
We advocated for the repeal of the previous Digital Security Act (DSA) of 2018 due to its provisions criminalizing free speech. While the Cyber Security Act (CSA) replaced the DSA in 2023, it retains many concerning aspects of the original law. We believe these provisions are incompatible with the CSA's stated purpose: to strengthen cyber security and address cybercrime.
We advocate for a redrafted CSA that incorporates recommendations from experts and human rights organizations and incorporates best practices to create a robust cyber security framework. Ideally, the Cyber Security Rules should have been formulated after such a redraft.

While the new Cyber Security Rules, 2024 is much appreciable, it perhaps does not reflect the government's positive political will as envisaged in various policy and strategy documents. The proposed Rules should be revisited with the following issues in contention:

- The CSA should get an effective organizational structure;
- Instead of establishing new DFLs, we should equip and enrich the existing one;
- The personal, educational and technical qualifications of cyber security personnel should be set by Rules;
- The Rules should incorporate forensic legal procedures to acquire data from local and foreign jurisdictions to ensure digital evidence admissibility in legal proceedings. At the same time, these procedures must comply with international human rights standards, particularly the right to privacy. The rules should ensure that individuals subject to cybersecurity investigations are afforded due process rights;
- The Rules could impact freedom of expression, particularly if they are used to justify broad monitoring or censorship. The Rules do not provide adequate protections for free speech and also do not recommend specific safeguards that prevent abuse of these powers under the guise of cybersecurity. Therefore, the Rules should incorporate human rights safeguards in the functioning of the CSA, NCERT and DFL.

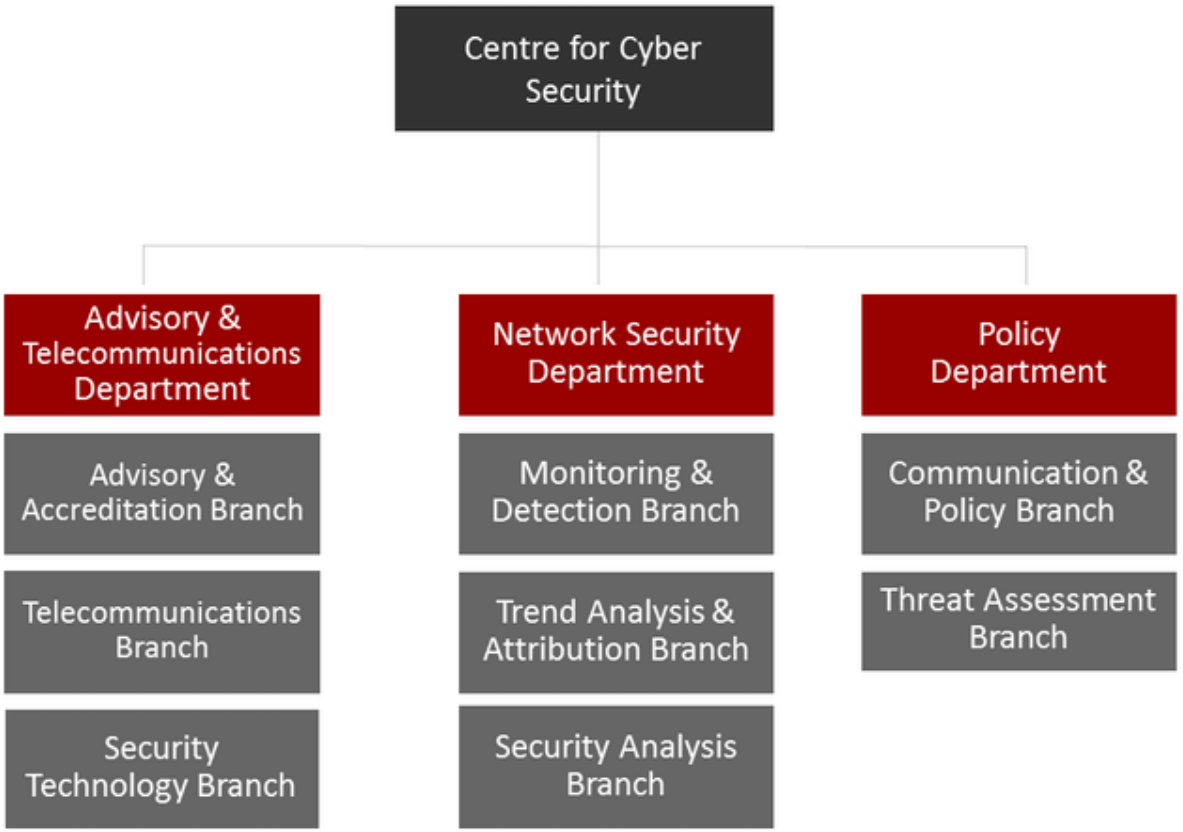
Annex 01

CISA: USA



Annex 02

Organizational Structure of the Danish Centre for Cyber Security[66]



[66] Source: CFCS, presentation given on 11 January 2016 (unpublished) (Available online at: https://www.researchgate.net/figure/Organizational-chart-of-the-Danish-Centre-for-Cyber-Security-Source-CFCS-presentation_fig3_309760543)

Annex 03

Source: **Acayo, Grace. (2017).** ***Global Cybersecurity Index Overview.*** **International Telecommunication Union, 2nd Annual Meeting of Community of Practice on Composite Indicators and Scoreboards (9-10 November 2017, Ispra, Italy), slide 5.**

Annex 04

Search List[67]

B.P. Form No. 44.
Bengal Form No. 5276.

Search List
[Regulation 260]
Details of property seized by Police Officers acting under the provisions of section 103 or 165, Criminal Procedure Code.

1. Date and hour of search .....

2. Name and residence of person whose house is searched .....

3. Name and residence of witness to search ..... { (1) ..... (2) ..... and so on .....

Serial No. (each article to be given a separate or collective serial).	Description of articles seized.	Description of place where article seized was found.	Name, father's name, residence, etc. of person or persons ordinarily occupying the house in which an article is seized.	Remarks (Here should be noted in the serial number in complainant's maltalika and the exact circumstances under which all articles have been found. A note should also be made in case anything unusual is observed, such as the remains of burnt paper, etc.)
1	2	3	4	5

K. B. - This form must be signed by witnesses.
" Articles seized, numbered and labeled should be attended by signature of witnesses and police officers.
Permanent marks, such as outs, etc, must not made.
Signature with date of the person whose properly seized if present at the search.

Signature of witness with date.
Signature by the accused (optional).
Police officers conduction the search.
Date..... Place.....

[67] https://www.police.gov.bd/en/police_forms?page=2#; https://pbi.gov.bd/pbi_hq/docs/english/BP44_property_seized.pdf

Annex 05

Comparison of Digital Evidence Admissibility Provisions in the Evidence Act of Bangladesh and India

Section	Bangladesh[68]	India[69]
65A	The contents of digital records may be proved in accordance with the provisions of section 65B	The contents of electronic records may be proved in accordance with the provisions of section 65B.
65B	(1) Notwithstanding anything contained in this Act, any information contained in a digital record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.	(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.
	(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:	(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: —
	(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes or any activities regularly carried on over that period by the person having lawful control over the use of the computer;	(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
	(b) during the said period, information of the kind contained in the digital record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;	(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
	(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the digital record or the accuracy of its contents; and	(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
	(d) the information contained in digital record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.	(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.
	(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether-	(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
	(a) by a combination of computers operating over that period; or	(a) by a combination of computers operating over that period; or
	(b) by different computers operating in succession over that period; or	(b) by different computers operating in succession over that period; or
	(c) by different combinations of computers operating in succession over that period; or	(c) by different combinations of computers operating in succession over that period; or
	(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,	(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

[68] Sections 65A and 65B were inserted by section 12 of the Evidence (Amendment) Act, 2022 (Act No XX of 2022).

[69] Sections 65A and 65B were inserted by section 92 and the Second Schedule of the Information Technology Act, 2000 (Act 21 of 2000).

	all the computers used for that purpose during that period shall be treated for the purposes of that section as constituting a single computer; and references in this section to a computer shall be construed accordingly.	all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
	(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate containing any of the following things, that is to say, -	(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, —
	(a) identifying the digital record containing the statement and describing the manner in which it was produced;	(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
	(b) giving such particulars of any device involved in production of that digital record as may be appropriate for the purpose of showing that the digital record was produced by a computer;	(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
	(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,	(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
	and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.	and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
	(5) For the purposes of this section, -	(5) For the purposes of this section, —
	(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;	(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
	(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to the computer, shall be taken to be supplied to it in the course of those activities;	(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
	(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.	(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
	Explanation: -For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.	Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.