TRANSPARENCY INTERNATIONAL BANGLADESH

Social movement against corruption

Digital Security Act 2018 and the draft Cyber Security Act 2023 : A Comparative Analysis

1. Background

Since its inception, the Digital Security Act 2018 (DSA) of Bangladesh has faced extensive criticism for being used as a tool against freedom of expression, media freedom, human rights, and dissension. On the other hand, it has been equally criticised for failing to ensure effective online safety, security of the digital system and protection of personal data and fundamental rights. The DSA's vague definitions of crimes and wide scopes of interpretation were used and abused for targeted criminalisation of free speech that not only caused immense suffering to the victims but also created an atmosphere of intimidation, self-censorship, and a sense of insecurity among people at large and media and civil society in particular. The decision to replace the DSA with a new draft Cyber Security Act (draft CSA) is an example of the Government's recognition that it was a black law that failed to find the right balance between digital security and civil liberties and compromised the latter in the name of the former.

The Constitution of the People's Republic of Bangladesh (art 39),[1] as in every other society that has embraced democracy and adhered to the rule of law throughout centuries, has guaranteed the freedom of speech and expression, thought and conscience and freedom of the press. Moreover, free speech is one of the most valued fundamental human rights in all free societies and is recognised in key international legal instruments, including the Declaration of the Rights of Man and the Citizen, 1789 (art 11),[2] the Universal Declaration of Human Rights (UDHR) 1948 (preamble, arts 18 & 19),[3] the International Covenant on Civil and Political Rights 1966 (ICCPR) (articles 18 & 19)[4] which Bangladesh has acceded to. The DSA has been considered to have contained many provisions that are contradictory to the Constitutional provisions as well as pledges under these international instruments. The following data will support the above statement.

1 http://bdlaws.minlaw.gov.bd/act-details-367.html.
2 https://constitutionnet.org/sites/default/files/declaration_of_the_rights_of_man_1789.pdf.
3 https://www.un.org/en/about-us/universal-declaration-of-human-rights.
4 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

1. From September 2018 until January 2023, over 7,001 cases have been filed across the country under the DSA[5] for exercising the right to free speech, dissenting voice, and independent media reporting.
2. The fate of most of the accused was left uncertain, as only 2 per cent of those accused under the DSA witnessed their cases resolved in court, resulting in being found guilty, declared not guilty, or having the cases dropped.[6]
3. Opposition politicians, journalists, businesspeople, students, and private employees were among the main victims of the DSA.[7]
4. Ruling party affiliates were the largest group prosecuting journalists.[8]
5. On average, a ruling party activist has filed a case every week over the last four years.[9]
6. One out of every three individuals facing charges under the DSA has been arrested.[10]
7. During these years, 60 per cent of cases were filed for Facebook activity.[11]
8. Between January 2020 and February 2022, approximately 2244 individuals faced charges in 890 cases, including 254 politicians and 207 journalists, with the majority of accusers being political party members (206), the Rapid Action Battalion (RAB, 87), and government officials (43).[12]

Due to the presence of vague and overly broad rules that criminalise various legitimate forms of expression and impose harsh penalties, including life imprisonment for repeated offenders, excessive police and DSA agency powers, and the existence of non-bailable offences and pre-trial detention, the UN Office of the High Commissioner for Human Rights (OHCHR) issued a Technical Note for the Government of Bangladesh in June 2022, recommending revisions to the DSA. Specifically, the OHCHR proposed the repeal or amendment of sections 8, 21, 27, 28, 29, 31, 32, 43, and 53 of the DSA.[13] The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression also called for repealing the DSA, highlighting concerns about arbitrary detention, torture, custodial death of journalists, and the chilling impact on journalism.[14] Moreover, the Editor's Council of Bangladesh,[15]

5 https://www.tbsnews.net/bangladesh/over-7000-cases-filed-under-dsa-law-minister-644486.
6 https://www.thedailystar.net/news/bangladesh/news/cases-under-dsa-almost-all-accused-kept-hanging-3221031.
7 https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951.
8 https://www.thedailystar.net/news/bangladesh/news/cases-under-dsa-almost-all-accused-kept-hanging-3221031.
9 Ibid.
10 Ibid.
11 Ibid.
12 https://freedominfo.net/dsa/media/documents/3a02ffb2-3bc8-46f2-abbd-d72f8f837b72.pdf
13 https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf.
14 https://www.dhakatribune.com/bangladesh/274568/digital-security-act-a-tool-for-harassment.
15 https://www.thedailystar.net/news/bangladesh/news/repeal-dsa-amend-all-anti-free-press-laws-3309506.

Transparency International Bangladesh (TIB),[16] Amnesty International,[17] European diplomats in Bangladesh,[18] and many other organisations have consistently called for repealing the DSA due to its potential misuse of free speech.

Transparency International Bangladesh (TIB) has been at the forefront of advocating for the repeal of the Digital Security Act, highlighting a multi-faceted critique that extends beyond human rights abuses. While TIB recognised and condemned the law's infringement upon human rights and freedom of expression, it also delved into the law's fundamental conceptual flaws. TIB emphasised that the law disproportionately focuses on addressing cybercrimes rather than fostering comprehensive cyber security.

In response to the mounting national demands and international critique, on 7 August 2023, the Cabinet of Bangladesh decided to replace the contentious Digital Security Act 2018 (DSA) with the draft Cyber Security Act 2023 (draft CSA). The decision raised the expectation that the era of the DSA would conclude. Unlike the DSA, the proposed draft CSA would focus on the core and specific mandate of ensuring cyber security as per international practice instead of being another tool to restrict free speech and other rights. However, upon closer examination of the DSA and draft CSA, it has become clear, as detailed below, that the draft CSA approved on 28 August 2023 contains hardly any change compared to the DSA except the title containing all its repressive provisions with only minor changes in punishment in a few cases.

2. Comparative Discussion between DSA and draft CSA

SL	Section, sub-section	Subject Matter	DSA	Draft CSA	Comments
1.	From the preambular clauses to section 2(g) of the draft CSA, there is no new content, apart from the verbatim text borrowed from the DSA and the substitution of the term 'Digital Security Act' with 'Draft Cyber Security Act'.				
2.	2(h)	Definition of NCERT (National Computer Emergency Response Team) in the DSA	There was no definition of NCERT (National Computer Emergency Response Team) in the DSA	Draft CSA defines NCERT in the following way: "National Computer Emergency Response Team" means the National Computer	The inclusion of this was needless in the draft CSA since it could have been addressed by

16 https://www.ti-bangladesh.org/articles/story/6698.
17 https://www.amnesty.org/en/documents/asa13/4514/2021/en/; https://www.amnesty.org/en/petition/stop-crackdown-on-freedom-of-expression-online-in-bangladesh/.
18 https://www.forbes.com/sites/emmawoollacott/2018/09/28/bangladeshi-digital-security-act-draws-fire-from-eu/?sh=6e0dd0916027.

				Emergency Response Team or Computer Emergency Response Team formed under section 9	inserting the term 'National' before the definition of the 'Computer Emergency Response Team' in section 2(d) of the draft CSA.
3.	2(i) to 2(v)	There are no changes in the rest of the definition clause except for substituting DSA with draft CSA.	In sections 2(i) to 2(v), there are no additional inclusions in the draft CSA apart from the direct insertion of the DSA's text.	2(i) to 2(v)	There are no changes in the rest of the definition clause except for substituting DSA with draft CSA.
4.	3-9	No significant changes in sections 3 to 9	In sections 3 to 9, there is no significant change in the draft CSA other than inserting the texts of the DSA verbatim and the use of the term 'National' on two occasions, i.e., sections 9(3) and 9(4), with a reference of the term 'computer incident response team' once in section 9(5) of the draft CSA.		
5.	10-16	No significant changes in sections 10-16	The provisions of sections 10 to 16 of the draft CSA have remained unchanged compared to the DSA, except for the modification of 'Digital Security Council' to 'Cyber Security Council' in section 12. Additionally, unlike the DSA, the draft CSA includes the names of officials such as the Director General of the Directorate General of Forces Intelligence (DGFI), Director General of the Directorate General of National Security Intelligence (NSI), Director General of the National Telecommunication Monitoring Centre (NTMC), and Director General of the National Cyber Security Agency as members of the National Cyber Security Council formed under section 12 of the draft CSA.		
6.	17	Punishment for illegal access to any critical information infrastructure, etc.	7 (seven) years imprisonment and a fine of taka 25 (twenty-five) lac is available in both DSA and draft CSA.	Under this section, the punishments include 3 (three) years imprisonment. However, more severe punishments for second-time offences have been removed.	Four years less imprisonment in the draft CSA

7.	18	Illegal access to computers, digital devices, computer systems, etc. and Punishment	The exact punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
8.	19	Damage to computer, computer system, etc. and punishment	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
9.	20	Offence and punishment related to modification of computer source code	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
10.	21	Punishment for making any propaganda or campaign against liberation war, the spirit of the liberation war, father of the nation, the national anthem or national flag	10 (ten) years imprisonment, or with a fine not exceeding Taka 1 (one) crore, or with both.	The penalty includes 5 (five) years of imprisonment, a fine not exceeding Taka one crore, or both. Furthermore, the draft CSA does not incorporate the more severe penalties for repeated offences.	The draft CSA imposes a shorter prison term of 5 (five) years and does not introduce additional penalties for repeated offences.
11.	22	Punishment for digital or electronic forgery	5 (five) years imprisonment, or with a fine not exceeding Taka 5 (five) lac, or with both.	The draft CSA entails a prison term of 2 (two) years, a fine not exceeding Taka 5 (five) lacs or both. Notably, the draft CSA omits more stringent penalties for repeated offences.	The draft CSA imposes a shorter prison term of 3 (three) years and does not introduce additional penalties for repeated offences.

12.	23	Punishment for digital or electronic fraud	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
13.	24	Punishment for identity fraud or personation.	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
14.	25	Punishment for transmission, publication, etc., of offensive, false or threatening data information	3 (three) years imprisonment, or with a fine not exceeding taka 3 (three) lac, or with both.	The draft CSA stipulates a potential imprisonment of 2 (two) years, a fine not exceeding Taka 3 (three) lac, or both. Nevertheless, the draft CSA has eliminated harsher penalties for repeated offences.	The draft CSA entails 1 (one) year less of imprisonment and does not introduce additional penalties for a second-time offence.
15.	26	Punishment for unauthorised collection, use, etc., of identity information	5 (five) years imprisonment, or with a fine not exceeding taka 5 (five) lac, or with both.	The draft CSA stipulates a 2 (two)-year imprisonment term or a fine not exceeding taka five lacs or both. However, the draft CSA does not include more severe penalties for a second-time offence.	The draft CSA imposes a reduced imprisonment term of 3 (three) years and does not entail additional penalties for a second-time offence.
16.	27	Offence and punishment for committing cyberterrorism	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
17.	28	Punishment for publication, broadcast, etc., of information on the website or in any	5 (five) years imprisonment, or with a fine not exceeding taka 10 (ten) lac, or with both.	The draft CSA imposes a fine not exceeding taka five lacs. However, the draft CSA does not include more severe penalties for a second-time offence.	The draft CSA does not impose any imprisonment under this section and does not entail additional penalties for a

		electronic format that hurts the religious values or sentiment			second-time offence.
18.	29	Punishment for publication, transmission, etc., of defamatory information	3 (three) years imprisonment, or with a fine not exceeding taka 5 (five) lac, or with both.	A fine not exceeding taka 25 (twenty-five) lacs is prescribed under the draft CSA, but more severe penalties for a second-time offence have been eliminated.	The possibility of imposing an additional fine of 20 (twenty) lacs along with the potential for imprisonment exists in the draft CSA, though the imprisonment term is not specified.
19.	30	Offence and punishment for e-transaction without legal authority	5 (five) years imprisonment, or with a fine not exceeding taka 5 (five) lac, or with both.	The draft CSA stipulates a fine not exceeding taka 25 (twenty-five) lacs or a combination of fines and other penalties. Nevertheless, the draft CSA does not include the more stringent punishments for a second offence that was present in the DSA.	The possibility of imposing an additional fine of 20 (twenty) lacs along with the potential for imprisonment exists in the draft CSA, though the imprisonment term is not specified.
20.	31	Offence and punishment for deteriorating law and order, etc.	7 (seven) years imprisonment, or with a fine not exceeding taka 5 (five) lac, or with both.	A sentence of 5 (five) years of imprisonment, or a fine not surpassing taka 25 (twenty-five) lac, or a combination of both, is specified in the draft CSA. Nonetheless, the draft CSA omits the imposition of harsher penalties for a second-time offence that existed in the previous legislation.	The draft CSA introduces a reduced prison term of 2 (two) years compared to the DSA, accompanied by an additional fine of 20 lacs.

21.	32	Offence and punishment for breaching the secrecy of the Government	14 (five) years imprisonment, or with a fine not exceeding taka 25 (twenty-five) lac, or with both.	The draft CSA stipulates a maximum imprisonment term of 7 years and a fine not exceeding taka 25 (twenty-five) lacs or both. Notably, the draft CSA does not include the harsher penalties for repeated offences that were present in the previous legislation.	The draft CSA imposes a reduced maximum imprisonment period of 7 years without any additional penalties for a repeated offence.
22.	33	Punishment for holding, transferring data information illegally, etc.	Section 33 of the DSA has been entirely omitted from the draft CSA.		
23.	34 (sec 33, draft CSA)	Punishment for an offence related to hacking and punishment thereof	The same punishments are present in the DSA and draft CSA; however, the draft CSA no longer includes the more severe penalties for repeated offences.		
24.	35-39 (secs 34-38, draft CSA)	There have been no modifications in the headings, subheadings, content, or provisions within the designated sections of the DSA and the draft CSA. The texts in these sections remain identical.			
25.	40 (sec 39, draft CSA)	The time limit for investigation, etc.	The Investigation Officer is required to conclude the investigation within 60 days from the initiation of the investigation under the DSA.	The draft CSA permits 90 days from the commencement of the investigation	
26.	41-49 (secs 40-48, draft CSA)	There have been no modifications in the headings, subheadings, content, or provisions within the designated sections of the DSA and the draft CSA. The texts in these sections remain identical.			
27.	50	Application of the Code of Criminal Procedure	The Code of Criminal Procedure (Cr. PC) applied to the investigation, trial, appeal,	In contrast, the draft CSA requires compliance with the regulations specified in	

	(sec 49, draft CSA)		and associated matters concerning any offence under the DSA as long as it did not conflict with the provisions of this Act.	sections 2 and 3 of Chapter 8 of the Information and Communication Technology Act, 2006, in addition to the utilisation of the Code of Criminal Procedure (Cr. PC).	
28.	51-52 (sec 50-51, draft CSA)	There have been no modifications in the headings, subheadings, content, or provisions within the designated sections of the DSA and the draft CSA. The texts in these sections remain identical.			
29.	53 (sec 52, draft CSA)	Offences to be cognisable and bailable	The DSA delineated in sections 17, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31, 32, 33, and 34 will be deemed cognisable and non-bailable. The enactment outlined in sections 18(1)(b), 20, 25, 29, and 47(3) will be considered non-cognisable and bailable.	The draft CSA outlined in sections 17, 19 and 33 will be classified as cognisable and non-bailable Offences. The Act stipulated in sections 18(1)(b), 20, 21, 22, 23, 24, 25, 26, 28, 29, 31, 32 and 46 will be designated non-cognisable and bailable Offences. The actions detailed in section 18(1)(a) are considered non-cognisable and bailable and can be resolved with the court's approval.	In the DSA, there were 14 sections where offences were classified as both cognisable and non-bailable. However, in the draft CSA, there are 3 sections where Offences are categorised as cognisable and non-bailable.
30.	54-56 (sec 53-55, draft CSA)	There have been no modifications in the headings, subheadings, content, or provisions within the designated sections of the DSA and the draft CSA. The texts in these sections remain identical.			

31.	57, DSA	Actions are taken in good faith	No suit or prosecution or any other legal proceeding shall lie against any employee or person concerned for any damage caused or likely to be caused to any person consequent to anything which is done in good faith under the DSA.	Section 57 of the DSA has been entirely omitted from the draft CSA.	Section 57 of the DSA has been entirely omitted from the draft CSA.
32.	58-62 (sec 56-60, draft CSA)	There have been no modifications in the headings, subheadings, content, or provisions within the designated sections of the DSA and the draft CSA. The texts in these sections remain identical.			

3. Summary

Based on the above comparative discussion, the following findings are evident:

1. The draft CSA is essentially a renamed version of the DSA, with only a few alterations in the form of apparently reduced severity of punishments. For example, the draft CSA does not provide for punishments for committing an offence a second time in some instances.
2. In certain sections, the draft CSA provides shorter imprisonment sentences compared to the DSA, though it proposes higher fines than the DSA in several sections.
3. The time allowed to complete the investigation under the draft CSA as per section 39 (DSA 40) has been extended to 90 days instead of 60.
4. The draft CSA has more non-cognisable and bailable sections than the DSA.
5. In substance, the draft CSA contains all the provisions from the DSA that compromise freedom of speech, dissent, thought and conscience, freedom of the press, and independent journalism.

4. General Discussion: Cybersecurity, Cybercrime, and Cyber Security Law

In reaction to protests and criticism, the government chose to replace the DSA with the draft Cyber Security Act (draft CSA) after five years. The Cabinet recently approved the draft CSA draft after incorporating further adjustments in two sections in the first draft. The government aims to pass the draft CSA in the upcoming September parliamentary session.[19] However, a meticulous examination of the draft Act reveals crucial misconceptions, challenges linked to free speech, and notable gaps in establishing a robust cyber security framework.

4.1. Essence of Cyber Security and Cybercrime

Cyber security encompasses a holistic set of measures aimed at safeguarding digital systems, networks, data, and critical infrastructure from cyber threats and unauthorised access.[20] It involves proactive strategies like risk assessment, vulnerability management, incident response planning, and continuous monitoring to ensure the confidentiality, integrity, and availability of digital assets.[21]

On the other hand, cybercrimes refer to unlawful activities carried out in the digital domain, such as hacking, data breaches, online fraud, and identity theft.[22] These activities are targeted at exploiting vulnerabilities in digital systems, causing financial losses, compromising sensitive information, and disrupting digital operations.[23]

4.2. Combining Cyber Security and Cybercrimes: A Problematic Approach

The naming of the draft Cyber Security Act (draft CSA) suggests a focus on safeguarding digital infrastructure and systems from cyber threats. However, the inclusion of cybercrimes within the same legislation, as indicated in the preamble, can create a misleading and problematic legal framework. Such a combined approach presents several challenges:

[19] https://www.thedailystar.net/news/bangladesh/governance/news/cyber-security-act-cabinet-gives-final-approval-3405326
[20] https://www.nist.gov/cyberframework
[21] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[22] https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html
[23] https://www.interpol.int/en/Crimes/Cybercrime

(a) Diluted Focus on Cyber Security: The combination of cyber security and cybercrimes in a single legislation may inadvertently lead to an imbalanced focus, with more attention directed towards punitive measures against cybercrimes rather than preventive measures to enhance overall cyber security.[24]

(b) Ambiguous Legal Provisions: A unified legislation risks creating legal provisions that are either ambiguous or conflicting. Cyber security and cybercrime laws necessitate distinct approaches; merging them can lead to complexities in drafting and interpreting legal provisions.[25]

(c) Inadequate Attention to Cyber Security Measures: Focusing heavily on cybercrimes might overshadow the importance of proactive cyber security measures. Effective cyber security strategies require continuous efforts in risk management, mitigation, and resilience building.[26]

(d) Misalignment with International Norms: The global landscape demonstrates the separation of cyber security and cybercrime laws. For example, the European Union's General Data Protection Regulation (GDPR) focuses on data protection, while the Convention on Cybercrime (Budapest Convention) specifically addresses cybercrimes.[27] This separation facilitates international cooperation and alignment with established norms.[28]

(e) Encouraging Multi-Stakeholder Cooperation: A dedicated cyber security legislation encourages collaboration between government entities, private sector stakeholders, academia, and civil society, fostering a holistic approach to enhancing digital resilience.

(f) Clarity of Legislative Objectives: Combined legislation might result in ambiguity regarding the primary legislative objectives, making it challenging for stakeholders to discern whether the law prioritises preventive cyber security measures or punitive actions against cybercriminals.

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[25] https://www.wto.org/english/tratop_e/msmes_e/uncitral_240621.pdf
[26] https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration
[27] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[28] https://hcss.nl/gcsc-norms/

The complexities arising from the amalgamation of cyber security and cybercrimes within the draft Cyber Security Act (draft CSA) are not unforeseen, as they closely mirror the provisions of the Digital Security Act (DSA). The challenges discussed earlier are indeed reflected in the draft CSA, echoing the concerns that have arisen with the DSA's implementation.

4.3. Components of Cyber Security Law

In the ever-evolving landscape of digital threats, crafting an effective cyber security law is paramount to safeguarding both individuals and organisations from cyberattacks. A comprehensive approach to cyber security should encompass a balanced combination of technological solutions and human expertise, recognising that neither can function optimally in isolation. Drawing inspiration from global jurisdictions, a robust cybersecurity law should incorporate the following components:

4.3.1. Technological Solutions

Embracing cutting-edge technologies is imperative in fortifying cyber defences. These solutions encompass various aspects of prevention, detection, mitigation, and recovery:

a. Encryption and Data Protection: Implementing robust encryption mechanisms safeguards sensitive information from unauthorised access, bolstering data privacy.[29][30]

b. Intrusion Detection and Prevention Systems (IDPS): Sophisticated IDPS platforms continuously monitor network traffic to identify and thwart potential intrusions, minimising vulnerabilities.[31]

c. Security Information and Event Management (SIEM) Systems: SIEM solutions consolidate and analyse security event data, facilitating rapid response to potential threats.[32]

[29] https://gdpr-info.eu/
[30] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
[31] https://www.cisa.gov/sites/default/files/publications/ncps-intrusiondetection-pia-092019.pdf
[32] https://www.draft CSA.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

d. Multi-Factor Authentication (MFA): Enforcing MFA strengthens authentication processes, reducing the risk of unauthorised access to systems and data.[33]

4.3.2. Human Expertise

While technology is pivotal, human expertise plays a vital role in interpreting complex cyber threats, strategising responses, and ensuring ethical considerations are met:

a. Skilled Workforce Development: Investing in cyber security education and training programs cultivates a skilled workforce capable of identifying and addressing emerging threats.[3435]

b. Collaboration and Information **Sharing:** Fostering collaboration among government agencies, private sector entities, and international partners enhances threat intelligence and effective incident response.[36]

c. Legal and Ethical Considerations: Human experts are essential in assessing the legal and ethical implications of cyber security measures, ensuring compliance with human rights and privacy standards.[37]

d. Public Awareness and Education: Raising public awareness about cyber threats empowers individuals to adopt safe online practices, contributing to a cyber-resilient society.[38]

4.3.3. International Cooperation

Cyber threats transcend national borders, necessitating international collaboration and adherence to global norms and standards:

[33] https://pages.nist.gov/800-63-3/sp800-63b.html
[34] https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education
[35] https://www.ncsc.gov.uk/report/decrypting-diversity-2021-diversity-and-inclusion-in-cyber-security
[36] https://www.cyber.gov.au/sites/default/files/2023-03/cima_2018_a4.pdf
[37] https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[38] https://csrc.nist.gov/pubs/sp/800/181/r1/final

a. International Agreements and Conventions: Participation in international agreements, such as the Budapest Convention on Cybercrime, fosters cooperation among nations to combat cybercriminal activities.[39]

b. Harmonization of Laws and Regulations: Efforts to align cyber security laws with global standards enable consistent legal frameworks, facilitating international cooperation in combating cyber threats.[40]

c. Cyber Diplomacy: Engaging in cyber diplomacy strengthens international relations, promotes responsible behaviour in cyberspace, and facilitates cooperation in addressing common challenges.[41]

It is imperative that a holistic cyber security law must integrate technological solutions with human expertise underpinned by international cooperation. As threats evolve, policymakers should draw inspiration from diverse global approaches to establish a comprehensive framework that safeguards digital ecosystems while upholding individual rights and privacy.

4.4. Content Moderation

Content moderation and cybersecurity are distinct concepts that serve different purposes. Content moderation involves the removal or restriction of online content that violates platform rules or community guidelines, while cybersecurity laws focus on protecting computer systems, networks, and data from unauthorised access, attacks, and breaches. Including content moderation within cybersecurity laws can raise concerns about freedom of expression and effective regulation. Here are some reasons why content moderation should not be included in cybersecurity laws, along with references:

a. Freedom of Expression Concerns: Content moderation often involves decisions about what content is allowed or prohibited on online platforms. Placing these decisions under cyber security laws might lead to the suppression of legitimate expression and could have a chilling effect on users' freedom of speech.[42]

b. Blurred Focus and Overreach: Cyber security laws primarily aim to safeguard the integrity and security of digital systems. Combining content moderation with cyber security measures could lead to a lack of focus on cyber security issues, potentially resulting in overbroad regulations that cover both security and content concerns.[43]

[39] https://rm.coe.int/1680081561
[40] https://www.weforum.org/reports/cybercrime-prevention-principles-for-internet-service-providers/
[41] https://dig.watch/resource/un-gge-report-2015-a70174
[42] https://opennet.net/research/publications/content-filtering-and-global-politics-internet
[43] https://cdt.org/insight/cdts-internet-security-and-free-expression-project-principles-for-regulation-of-content-moderation-practices/

c. Legal Uncertainty: Content moderation involves complex legal and policy considerations related to freedom of expression, privacy, and intermediary liability. Embedding content moderation within cyber security laws could create legal ambiguity and confusion, as the focus on security may not adequately address these broader concerns.[44]

d. Risk of Over-Censorship: Combining content moderation with cyber security measures might incentivise online platforms to err on the side of caution and remove content to avoid legal risks. This could result in over-censorship of lawful speech to prevent potential cyber security violations.[45]

e. Diverse Jurisdictions and Cultural Differences: Different countries have varying legal standards and cultural norms concerning acceptable online content. Embedding content moderation within cyber security laws may not account for these differences and could lead to conflicting and inconsistent regulations.[46]

f. Limitation of Resources: Cyber security agencies often have a primary focus on preventing and mitigating cyber threats. Adding content moderation responsibilities to their mandate could divert resources away from addressing critical cyber security issues.[47]

4.5. Rethinking the Scope and Contents of Cyber Security Law

The integration of speech-related offences such as the criminalisation of speech, hostile speech, false information provisions, and defamation within cyber security law raises profound concerns about freedom of expression and the diversion of legal resources from addressing actual cybercrimes. The focus on these elements not only undermines the core principles of free speech but also poses a threat to the effective enforcement of cyber security in its true sense.

a. **Threat to Freedom of Expression:** Incorporating provisions criminalising speech, hostile speech, and defamation within cyber security law can lead to an undue restriction on the right to freedom of expression. This fundamental human right,

[44] https://www.eff.org/issues/intermediary-liability
[45] https://www.article19.org/resources/content-moderation-and-freedom-of-expression-a-comparative-tool/
[46] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session17/Documents/A.HRC.17.27_en.pdf
[47] https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

enshrined in the Constitution of Bangladesh and international standards, ensures citizens' ability to voice their opinions without fear of censorship or reprisal.[4849]

b. **Chilling Effect and Self-Censorship**: The inclusion of overly broad provisions against hostile speech and defamation risks creating a chilling effect on public discourse. Individuals and media outlets may self-censor to avoid legal repercussions, hindering the open exchange of ideas and essential democratic discussions.[50]

c. **Diversion of Resources:** By incorporating speech-related offences as cybercrimes, the judiciary and law enforcement agencies may be consumed with addressing speech-related cases rather than focusing on actual cybercrimes that involve hacking, data breaches, and online fraud. This diverts essential resources from combating cyber threats that directly compromise cyber security.

d. **Erosion of Judicial Independence:** The heavy caseload of speech-related offences within the cyber security framework may result in overburdened courts and strain the judicial system. This, in turn, may affect judicial independence and due process as time and resources needed for adjudicating genuine cybercrime cases become scarce.

e. **Definition of Cybercrimes:** Cybercrimes typically encompass offences involving hacking, data breaches, identity theft, online fraud, and attacks on critical information infrastructure. The integration of speech-related offences within the cyber security framework blurs the line between actual cybercrimes and speech-related issues, causing confusion in enforcement and diminishing the effectiveness of addressing real threats.

f. **International Jurisdictions:** Numerous countries emphasise the separation of cybercrimes and speech-related offences. For instance, the European Union's General Data Protection Regulation (GDPR) prioritises data protection, while the Convention on Cybercrime (Budapest Convention) specifically addresses cybercrimes. This dual-focus approach recognises the distinct nature of these issues and ensures a comprehensive legal framework.[5152]

g. **Balancing Freedom of Expression and Security:** To truly secure the digital landscape, a holistic approach is needed—one that recognises the unique challenges posed by cybercrimes and the vital importance of protecting freedom of expression.

[48] http://bdlaws.minlaw.gov.bd/act-367.html
[49] https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[50] https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
[51] https://gdpr-info.eu/
[52] https://rm.coe.int/1680081561

This approach will lead to a robust and balanced legal framework that safeguards both security and individual rights, ensuring a safer digital environment for all.

h. **International Principles:** The International Principles on the Application of Human Rights to Communications Surveillance (IPCCR) underscores the necessity of safeguarding individuals' rights to privacy and freedom of expression in the digital realm. It emphasises the importance of ensuring that any limitations on these rights are prescribed by law, necessary, proportionate, and subject to effective oversight.[53]

4.6. Judicial Oversight

Ensuring effective judicial oversight in cyber security and cybercrime laws is essential to balance security imperatives with the protection of individual rights. Several mechanisms can be employed to achieve this goal:

a. **Clear Legal Frameworks:** Craft cyber security and cybercrime laws with clear and specific provisions that outline the scope, limitations, and procedures for law enforcement actions. These laws should incorporate safeguards to prevent abuse of power and ensure that judicial authorisation is required for intrusive measures.

b. **Judicial Authorisation:** Require law enforcement agencies to seek judicial authorisation before conducting intrusive actions such as surveillance, data interception, or searches. This ensures that an independent judicial body reviews and approves these actions based on legal standards. For example, the EU's ePrivacy Directive requires judicial authorisation for intercepting communications.[54]

c. **Transparency and Reporting:** Establish mechanisms for law enforcement agencies to report to the judiciary on the actions they have taken under cyber security or cybercrime laws. This allows the judiciary to monitor the use of these powers and intervene if necessary. The U.S. Foreign Intelligence Surveillance Court (FISC) reviews government surveillance requests and publishes annual reports on its activities.[55][56]

d. **Independent Oversight Bodies:** Create independent oversight bodies composed of legal and technical experts to review and audit law enforcement actions under cyber security laws. These bodies can assess whether actions were conducted in compliance

[53] https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf
[54] https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_en.pdf
[55] https://www.law.cornell.edu/uscode/text/50/1803
[56] https://www.law.cornell.edu/uscode/text/50/1871

with the law and recommend corrective measures if needed. The UK's Investigatory Powers Commissioner's Office (IPCO) oversees the use of surveillance powers.[57]

e. Judicial Training: Provide training to judges on technical aspects of cyber security and cybercrime. This empowers them to make informed decisions and understand the implications of their rulings. The Council of Europe provides resources and training for judges on cybercrime-related issues.[58]

f. Adversarial Process: Encourage an adversarial process where individuals affected by law enforcement actions have the opportunity to challenge those actions in court. This allows for a balanced assessment of the legality and proportionality of such actions. The U.S. Foreign Intelligence Surveillance Court of Review allows for appeals by aggrieved parties.[5960]

g. International Human Rights Standards: Align cyber security and cybercrime laws with international human rights standards, such as those outlined in the International Covenant on Civil and Political Rights (ICCPR). These standards emphasise the importance of judicial oversight in ensuring that limitations on rights are necessary, proportionate, and subject to review.[61]

Including provisions that allow the judiciary to consider expert opinions as evidence can significantly enhance the effectiveness of judicial oversight in cyber security and cybercrime cases. Expert opinions can provide valuable technical insights and context to judges who may not have specialised knowledge in these areas.

h. Expert Witness Testimony: Cyber security and cybercrime cases may involve complex technical concepts and intricacies that are beyond the expertise of judges. Allowing expert witnesses to testify can help elucidate technical matters for the court. For instance, an expert in digital forensics could explain the methods used to trace the origin of a cyber attack.

i. Technical Reports: Cyber security incidents often leave digital footprints that require technical analysis to interpret. Allowing technical reports prepared by experts to be submitted as evidence can provide judges with a detailed understanding of the events and help them make informed decisions. These reports could detail the nature of a cyber threat, the methods employed, and the potential impact.

[57] https://www.legislation.gov.uk/ukpga/2016/25/part/8/chapter/1/enacted
[58] https://www.coe.int/en/web/cybercrime/octopus_online_training_platform
[59] https://www.law.cornell.edu/uscode/text/50/1803
[60] https://www.supremecourt.gov/DocketPDF/20/20-1499/188774/20210827173144842_20-1499%20ACLU%20Opp.pdf
[61] https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf

j. **Advisory Role:** In cases where the judge lacks sufficient technical expertise, provisions can be established to seek advisory opinions from independent experts. These opinions would not be binding, but they would aid the court in making well-informed decisions. The EU's Network and Information Security Directive (NISD) encourages member states to establish Computer Security Incident Response Teams (CSIRTs) that can provide advice to authorities on cyber security matters.[62]

k. **Peer Review:** Establish mechanisms for expert opinions to undergo peer review by other experts. This adds an additional layer of validation and ensures the accuracy and credibility of the technical information provided to the court.

l. **Code of Conduct:** Ensure that expert witnesses adhere to a code of conduct that emphasises impartiality, accuracy, and ethical considerations. This maintains the integrity of the expert's role and the credibility of their testimony.

m. **Legal Qualifications:** Specify the qualifications that an expert witness should possess to testify in court. This could include certifications, experience, and recognised expertise in relevant fields.

4.7 Safeguarding Individual Rights: Limiting Broad Powers of Police Investigators in Cyber Security Law

In the context of cyber security law, the issue of granting broad powers to police investigators is a delicate balance between protecting national security and safeguarding individual rights. While law enforcement agencies play a crucial role in tackling cyber threats, it is imperative to ensure that their powers are carefully circumscribed to prevent overreach, abuses, and violations of privacy. This principle holds true across various jurisdictions, as evidenced by international standards and legal frameworks.

a. **Striking the Balance:** Granting broad powers to police investigators under cyber security laws may risk infringing upon citizens' fundamental rights, such as the right to privacy and freedom of expression. Striking the right balance between combating cyber threats and respecting individual rights requires clear limitations on the scope and application of investigative powers.[63]

b. **International Jurisdictions:** Numerous countries have encountered challenges when dealing with broad investigatory powers in the realm of cyber security. For instance, the United States' debates over the scope of the USA PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA) underscore the need for oversight to prevent government overreach. Similarly, the United

[62] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
[63] https://www.eff.org/issues/national-security

Kingdom's Investigatory Powers Act, often referred to as the "Snooper's Charter," has faced criticism for its broad surveillance powers.[64][65]

c. **Technical Challenges:** Broad investigatory powers must also be considered in the context of technical feasibility. Cyber security incidents often involve complex digital footprints and encryption technologies that can hinder or complicate investigations. Law enforcement's capacity to comprehend and effectively investigate such incidents requires technical expertise and resources. Overreaching powers without corresponding technical capability can lead to ineffective investigations and unintended consequences.[66]

d. **Judicial Oversight:** To prevent abuse of broad investigatory powers, judicial oversight is paramount. Independent judges can assess the necessity, proportionality, and legality of the actions taken by law enforcement. Judicial oversight ensures that investigative actions are compliant with the law and do not disproportionately intrude upon individual privacy and rights.[67]

e. **Strengthening Cyber Security Laws:** Rather than solely relying on broad investigatory powers, cyber security laws should emphasise comprehensive and collaborative approaches that involve public-private partnerships, technical solutions, and international cooperation. Fostering cyber resilience through a combination of proactive measures and responsive strategies can yield more effective results in safeguarding both national security and individual rights.

5. Evaluating the Draft Cyber Security Act

We have provided a brief overview of key components essential to any effective cyber security law. Building upon this foundation, we will now analyse and assess the provisions outlined in the draft Cyber Security Act.

5.1. National Cyber Security Agency

The provisions outlined in sections 5, 6, and 7 of the draft Cyber Security Act pertain to the establishment, structure, and appointment of key personnel within the Cyber Security Agency. While these provisions are a step in the right direction towards establishing an

[64] https://www.congress.gov/bill/107th-congress/house-bill/3162
[65] https://www.legislation.gov.uk/ukpga/2016/25/contents
[66] https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities
[67] https://www.britannica.com/topic/judicial-review

agency responsible for cyber security in Bangladesh, a comprehensive analysis reveals areas that could benefit from further refinement and alignment with global best practices.

a. **Establishment of Agency (Section 5):** The establishment of a dedicated agency for cyber security is crucial for addressing evolving cyber threats. However, the scope and functions of the agency should be more explicitly defined within the Act itself. Additionally, the Act should lay out the agency's responsibilities, such as incident response, threat intelligence, and coordination with other relevant authorities, to ensure a comprehensive cyber security framework.

b. **Appointment and Expertise (Section 6):** The requirement for appointing the Director General and Directors with expertise in computer or cyber security is a positive step. However, the Act should further emphasise the importance of multidisciplinary expertise, including legal, technical, and policy skills. This ensures that the agency is equipped to tackle the diverse challenges of cyber security effectively.

c. **Manpower and Resources (Section 7):** While the provision allows the agency to appoint necessary employees, it lacks specificity regarding the types of roles required, such as cybersecurity analysts, incident responders, legal experts, and policy advisors. The Act could include a broader framework for the agency's organisational structure and required skill sets.

When considering global best practices, the establishment of a cyber security agency should be accompanied by a well-defined mandate that aligns with international standards. For instance, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) focuses on critical infrastructure protection, incident response, and threat intelligence.[68] The UK's National Cyber Security Centre (NCSC) has a comprehensive role in protecting the country's cyberspace.[69] These models emphasise a multidisciplinary approach, expertise, and clear mandates.

5.2. Preventive Measures

The provisions outlined in sections 8, 9, 10, and 11 of the draft Cyber Security Act pertain to preventive measures and capabilities such as data removal or blocking, emergency response, digital forensic labs, and quality control. While these provisions indicate an effort to

[68] https://www.cisa.gov/
[69] https://www.ncsc.gov.uk/

establish mechanisms for proactive cyber defence, a comprehensive analysis highlights both positive aspects and potential areas for further enhancement in line with global best practices.

a. Data Removal or Blocking (Section 8): The Act's provisions enable the removal or blocking of data information that poses a threat to digital security or public order. While such provisions could be essential in addressing immediate threats, the criteria and oversight mechanisms for determining what constitutes a threat should be well-defined to avoid potential misuse. Additionally, ensuring transparency in the decision-making process and mechanisms for appeal are important to prevent censorship.

This section at its current form raises concerns regarding its potential misuse, vagueness of terms, and potential impacts on freedom of expression.

ICCPR and International Standards:

The ICCPR emphasises that any interference with individuals' privacy rights, including data removal or blocking, must adhere to principles of legality, necessity, proportionality, and due process. These principles are aimed at ensuring that any action taken by authorities respects individual rights while maintaining the legitimate aims of cyber security. Provisions related to data removal or blocking should align with these international standards to prevent arbitrary or excessive infringements on rights.

Vagueness and Potential Misuse:

The language used in this section contains vague terms such as "threat to digital security," "solidarity," "financial activities," and "religious values." The lack of clear definitions for these terms creates ambiguity and a risk of broad interpretation by authorities. Such vagueness can lead to arbitrary decision-making and potential misuse of these provisions for suppressing legitimate online expression. The absence of objective standards for determining whether content actually poses a threat or hampers solidarity undermines the predictability required under international human rights law.

b. **Emergency Response (Section 9):** The establishment of a National Computer Emergency Response Team (NCERT) is a positive step for swift response to cyber incidents. However, the Act could provide more clarity on coordination mechanisms between the NCERT and other relevant agencies, such as law enforcement and critical infrastructure owners. Moreover, defining the scope and extent of authority during emergency situations is crucial.

c. **Digital Forensic Labs (Sections 10 and 11):** The provisions for digital forensic labs indicate the recognition of the importance of digital evidence in cybercrime investigations. Ensuring that these labs operate with qualified personnel, maintain data security,

and adhere to scientific standards is essential. However, the Act could specify the level of independence and impartiality of these labs, ensuring they are not solely under the control of any specific agency and maintain a balance between law enforcement and privacy considerations.

5.3. National Cyber Security Council

The provisions outlined in sections 12 - 14 establish the National Cyber Security Council, comprising various government officials and specialists, to oversee the implementation of the draft Cyber Security Act, which is a positive step towards enhancing cyber security efforts. However, certain aspects of the composition and authority of the Council warrant consideration in terms of the best practices for effective governance in the realm of cyber security.

The provision related to the National Cyber Security Council in the draft Cyber Security Act does include representation from various government agencies and ministries, but it falls short of reflecting the level of expert representation seen in organisations like the U.K.'s NCSC or the U.S.'s CISA. In these entities, a critical element is the integration of technical expertise and cross-sector collaboration, which enhances the effectiveness of cyber security efforts.

a. **Expertise and Representation:** While the draft Act's Council includes officials from key government bodies, such as the Ministry of Post, Telecommunication and Information Technology, the Ministry of Law, Justice and Parliamentary Affairs, and others, the expertise in cyber security might be better addressed with dedicated representatives from specialised entities. For example, the armed forces, intelligence agencies, and police chiefs may not possess the technical knowledge required to address cyber security challenges effectively.

b. **Authority and Independence:** The Council's role is substantial, including providing directions, advice and formulating policies for digital security. To ensure the Council's effectiveness, it should be granted sufficient authority and independence in decision-making while also being subject to appropriate oversight mechanisms.

c. **International Examples:** In the U.S., CISA includes experts with technical knowledge, as well as representatives from various sectors such as energy, finance, and telecommunications, ensuring a holistic approach.[70] Similarly, the U.K.'s NCSC consists of technical experts with hands-on experience in cyber security from both public and private sectors.[71] Countries like Estonia have

[70] https://www.cisa.gov/
[71] https://www.ncsc.gov.uk/

established a Cyber Security Council with members from academia, the IT industry, legal experts, and law enforcement. Such inclusion ensures a balanced representation of expertise.

5.4. Critical Information Infrastructure

The provision of Critical Information Infrastructure (CII) in the draft Cyber Security Act (Section 15 – 16) is a crucial component for safeguarding essential digital assets. However, while the provision recognises the significance of monitoring, inspection, and expertise, it falls short of fully addressing the comprehensive tech and human solutions that are expected in a robust cyber security law.

a. **Tech Solutions:** The provision acknowledges the need for monitoring, inspection, and safety of critical information infrastructure. However, it lacks specific provisions related to mandatory cyber security measures, incident response protocols, and technical standards that would enhance the protection of critical assets. For instance, the European Union's NIS Directive mandates operators of essential services to implement security measures and report incidents.[72] Similarly, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) develops and enforces security guidelines for critical infrastructure sectors.[73] These provisions go beyond mere monitoring and emphasise proactive cyber security measures.

b. **Human Solutions:** While the provision mentions the involvement of experts in digital security for conducting inspections, it does not elaborate on the role of specialised personnel in decision-making and strategic planning. A comprehensive cyber security law should encompass training, skill development, and the establishment of specialised teams capable of responding to emerging threats. For example, the U.S. FISMA emphasises the importance of a qualified and skilled cyber security workforce for federal agencies.[74]

To enhance the tech and human solutions within the provision of Critical Information Infrastructure, the draft Cyber Security Act could have incorporated requirements for mandatory cybersecurity measures, incident response plans, and adherence to

[72] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
[73] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
[74] https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act#:~:text=Overview,OMB%20in%20developing%20those%20policies.

technical standards. Additionally, the law could outline the establishment of specialized cybersecurity teams and emphasise training and skill development for personnel involved in protecting critical assets.

5.5. Offence and Punishment

The provided chapter of the draft Cyber Security Act outlines various offences and their associated punishments related to digital activities. While the Act aims to enhance digital security and curb cyber-crimes, it's essential to critically analyse the provisions in light of international human rights standards and global best practices to ensure that fundamental rights are upheld. Let's examine key aspects and potential concerns with reference to relevant international standards:

a. **Overbroad Restrictions on Expression:** The Act includes provisions that criminalise the publication or transmission of offensive, false, or threatening data information (Section 25) and content that hurts religious values or sentiments (Section 28). While curbing harmful content is important, these provisions must be carefully crafted to avoid vague terms that could lead to overbroad restrictions on freedom of expression. International human rights law, including the International Covenant on Civil and Political Rights (ICCPR), emphasises that restrictions on expression must be narrowly defined and proportionate to a legitimate aim.

b. **Criminalisation of Online Activities:** Some provisions criminalise actions that might not warrant severe criminal penalties, such as illegal access to computers, computer systems, or networks (Sections 17 and 18). Best practices suggest that penalties should be commensurate with the gravity of the offence and should not disproportionately restrict individual rights. Excessive criminalisation can have a chilling effect on legitimate online activities.

c. **Violation of Right to Privacy:** The Act addresses identity fraud or personation (Section 24) and unauthorised collection or use of identity information (Section 26). While the protection of identity information is important, these provisions should be analysed in light of the right to privacy. The collection and use of personal data should adhere to established data protection principles, and the Act should ensure that lawful authority is defined clearly to prevent abuse.

d. **Lack of Safeguards for Digital Rights:** The Act doesn't explicitly mention safeguards for digital rights, such as due process guarantees, safeguards against arbitrary arrest, and protection against unwarranted surveillance. It's crucial for legislation to establish mechanisms to protect individuals from abuse of power and ensure that legitimate digital activities are not unduly hindered.

e. **Compatibility with International Standards:** The Act should be assessed for compatibility with international human rights standards, particularly the ICCPR, which Bangladesh is a party to. International standards emphasise the protection of freedom of expression, right to privacy, and due process rights, even in the context of cyber security measures.

f. **Potential for Overreach and Disproportionate Punishments:** Some provisions, such as those related to cyber terrorism (Section 27) and hacking (Section 33), propose severe punishments, including 14 (fourteen) years imprisonment and hefty fines. Such penalties could deter cybersecurity professionals from conducting legitimate research or reporting vulnerabilities, hindering the overall security of digital systems.

Section 32 - Offence and Punishment for Breaching Secrecy of the Government:

This section addresses offences related to breaching the secrecy of the government. While protecting sensitive government information is essential, the Act should ensure that definitions are clear and well-defined to prevent overbroad interpretations. Restrictions on access to government information should be consistent with international standards on the right to information and government transparency. International standards emphasise that any restrictions on the right to information must be narrowly defined, necessary, and proportionate.

Section 29 - Publication, Transmission, etc. of Defamatory Information:

Defamation laws can be a contentious issue when applied to online content. It's important to strike a balance between protecting reputation and safeguarding freedom of expression. Any provisions related to defamation should be formulated with precision and clarity to avoid suppressing legitimate criticism or stifling public discourse. International standards stress that defamation laws should not result in undue limitations on free expression, and civil remedies should be preferred over criminal penalties.

In conclusion, a comprehensive analysis of these selected sections underscores the need for careful consideration and potential exclusion to ensure that the final Cyber Security Act of Bangladesh aligns with international human rights standards and global best practices, effectively fortifying digital security without compromising essential liberties.

5.6. Investigation of Offence and Trial

The sections of the draft Cyber Security Act (draft CSA) related to investigation and trial (sections 38 to 53) establish procedures for law enforcement agencies to investigate and prosecute cybercrimes. While these provisions aim to address cybercrimes effectively, they also raise concerns related to due process, privacy, and the balance between law enforcement powers and individual rights.

1. Investigation and Powers (Sections 38-42): The Act grants certain powers to the Investigation Officer for the investigation of cybercrimes, such as search and seizure of digital devices, data, and materials related to offences. While these powers are necessary for effective investigation, it's important to ensure that they are exercised with proper oversight and accountability to prevent misuse. The procedures for obtaining search warrants and conducting searches must be clearly defined, and there should be safeguards against potential abuse.

The provision that mandates any offence under the Draft Cyber Security Act to be investigated solely by a police officer (referred to as the Investigation Officer) raises potential concerns regarding the expertise required for handling cyber-related offences. While police officers play a vital role in law enforcement, cybercrimes often demand specialised technical knowledge and investigative skills beyond the scope of traditional law enforcement.

a. **Lack of Technical Expertise:** Cybercrimes involve intricate digital mechanisms, data breaches, and sophisticated online activities that require a deep understanding of digital forensics and cyber techniques. Traditional police officers might not possess the technical proficiency needed to investigate and gather evidence in the digital realm effectively.

b. **Complex Investigations:** Cybercrimes often transcend geographical boundaries and involve multiple layers of virtual communication. Effective investigation in such cases requires collaboration with international law enforcement agencies, cyber security experts, and digital forensics specialists who can navigate the complexities of digital footprints.

   Sections 40, 45, and 46 confer the police investigator with overly broad powers that risk being misused and abused. The absence of an independent judicial oversight mechanism for the process of seizing computers and personal property adds to this concern. These provisions lack clear standards and can be invoked under the vague criterion of "investigation," which lacks a precise definition. The current provisions grant substantial discretionary authority to compel cooperation from individuals, entities, or service providers, as well as to confiscate private property, all without adequate safeguards, thereby failing the proportionality principle outlined in Article 19 of ICCPR. These provisions fall short of meeting the criteria necessary for permissible restrictions on the right to privacy.

Regarding the authority for search, seizure, and arrest with and without warrant, the existing regulations in Sect. 41 and Sect. 42 remain unchanged from the DSA. Sect. 41 mandates obtaining a warrant when there's reason to believe that an offence has been or will be committed under the Act, or if relevant data or evidence is held by any individual or entity. Meanwhile, Sect. 42 permits search, seizure, or arrest without a warrant when there's reason to believe that an offence has occurred or may occur, or if evidence could be tampered with or destroyed. These sections lack adequate safeguards to protect the rights to freedom of expression and privacy.

The thresholds required in Sect. 41 and 42 are unduly low, relying on "reasons" to believe an offence has or will occur, potentially leading to undue restrictions on freedom of expression. Additionally, both sections lack specificity on the criteria that must be satisfied before a warrant is issued, failing to provide meaningful judicial oversight. Furthermore, the scope of these provisions is overly broad, with no limitations on scope or duration. Such extensive powers to intercept, search, seize, and disclose information likely violate the right to privacy, as they allow the collection of wide-ranging categories of private data.

These sections, along with Sections 40, 45, and 46, lack essential guidelines for the conduct of search and seizure activities and fail to stipulate the return or destruction of seized equipment or data once investigations conclude. This gap raises significant concerns about the potential exposure of private data held by authorities. These provisions present a risk of misuse, particularly targeting activists and minority groups, thereby creating a chilling effect on freedom of expression and related rights.

6. Concluding Remarks

Some recent incidents underscore a glaring discrepancy between the aspirations of digital security measures and the reality of their implementation. Despite the existence of the Digital Security Act (DSA), the National Computer Incident Response Team (N-CIRT)[75], the National ICT Policy[76] and Cyber Security Strategy[77], a series of cyber-attacks, data leaks, and breaches have revealed the limitations of the current legal and technical framework in safeguarding digital assets and personal information. The incidents involving Biman Bangladesh Airlines[78], government institutions[79], and the leakage of sensitive personal data from the Office of the Registrar General, Birth & Death Registration[80] highlight the vulnerabilities that persist even under the existing security measures.

[75] https://www.cirt.gov.bd/
[76] https://www.cirt.gov.bd/wp-content/uploads/2019/11/ict-nitimala-2018.pdf
[77] https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/nothi_10314_2021_07_30_31627641428.pdf
[78] https://www.thedailystar.net/news/bangladesh/news/hackers-want-5m-biman-data-3279041
[79] https://www.thedailystar.net/news/bangladesh/crime-justice/news/websites-25-govt-private-institutions-hacked-3395101
[80] https://bdnews24.com/bangladesh/6yl7vppej6

The approval of the draft Cyber Security Act (draft CSA) with provisions similar to the DSA, despite the ongoing challenges, raises strategic questions about the direction of the nation's cybersecurity approach. The fact that the same provisions persist in the draft CSA suggests a continuity of approach that has not yielded the desired results thus far. The risk here is twofold: first, it could perpetuate the existing gaps and vulnerabilities that threat actors exploit, and second, it would continue to stifle the space for online freedom of expression due to the potential misuse of the repressive provisions, as evidenced by numerous cases filed under the DSA.

To navigate this complex landscape, a strategic shift is needed. This entails not just enacting legal frameworks but also aligning them with evolving cyber security threats and international human rights standards. A strategic approach should include provisions that prioritise proportionality, accountability, and judicial oversight while fostering collaboration between government agencies, private sector entities, and cyber security experts. Moreover, investing in cyber security education and workforce development is vital to bridge the technical gap and mitigate potential risks.

Ultimately, cyber security is a dynamic challenge that requires an adaptive and strategic response. Bangladesh has the opportunity to learn from the experience of DSA and adopt a more nuanced approach that not only safeguards digital infrastructure but also upholds citizens' rights. The strategic path forward lies in striking the right balance between security imperatives and the preservation of fundamental freedoms and in actively addressing the shortcomings that have hindered progress thus far.

In view of the above, TIB recommends that the draft CSA, as approved on 28 August, be thoroughly overhauled to prepare a genuine Cyber Security Act that will truly serve the purpose of ensuring the security of cyber infrastructure, computer and internet systems, digital platforms, and other components of the cyber system. The draft CSA should refrain from retaining any provisions from the DSA that compromise freedom of speech, dissent, thought and conscience, freedom of the press, and independent journalism. All stakeholders, including independent legal and technical experts, sector specialists with knowledge and expertise on international best practices, human rights organisations, journalists, and other relevant professionals, should be closely involved in the process of overhauling process of the draft.