USAID
FROM THE AMERICAN PEOPLE

COUNTERPART INTERNATIONAL
In partnership for results that last.

Handbook

Bangladesh's Cyber Security Act: A Guide for Civil Society, Media and the Public

OCTOBER 2024

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Handbook

Bangladesh's Cyber Security Act: A Guide for Civil Society, Media and the Public

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

This manual was made possible by the generous support of the American people through the United States Agency for International Development (USAID) under Cooperative Agreement No. 72038818CA00003 (Promoting Advocacy & Rights Activity). The opinions expressed herein are those of the author and do not necessarily reflect the views of Counterpart International or USAID/USG.

Published in October 2024

Table of Contents

1. Introduction

In 2023, the Government of Bangladesh enacted the Cyber Security Act (CSA) to regulate data security and activities online. The CSA replaced the controversial Digital Security Act 2018 (DSA), criticized by many domestic and international stakeholders as repressive, particularly for freedom of expression online.

The stated purpose of Bangladesh's Cyber Security Act of 2023 is to repeal the Digital Security Act, 2018 and to ensure cyber security by identifying, preventing, suppressing and prosecuting offences committed through digital or electronic means. The CSA retains much of the regulatory framework of the former DSA but has reduced the severity of most penalties.

The CSA has come under scrutiny for its similarity to the DSA, which was criticized for many provisions that violate international standards governing the freedom of expression, as well as its implementation, which has been marked by extensive use against journalists, civil society activists, and those critical of the government.[1] Concerns abound that the CSA will continue to restrict the freedom of expression online and curtail the right to privacy.

The purpose of this handbook is to provide an overview of the Cyber Security Act 2023 and its key provisions, as well as its application. The handbook also strives to provide a barometer of how the CSA measures up to international law governing the freedom of expression and other civic freedoms. Finally, because of the similarities between the previous DSA and the current CSA, this handbook contains some discussion on how the DSA has been implemented and its impact on civil society.

OBJECTIVES

- To raise awareness among civil society, media actors and the public of the contents of the Cyber Security Act 2023;
- To empower individuals, civil society and media actors to navigate the legal framework effectively.

1 Human Rights Watch. "Bangladesh: Events of 2021." Available at: https://www.hrw.org/world-report/2022/country-chapters/bangladesh.

2. Applicable International Legal Standards

The freedom of expression and the right to privacy are both guaranteed by the Universal Declaration of Human Rights, the International Covenant for Civil and Political Rights (ICCPR), and numerous other human rights conventions and declarations. Having acceded to the ICCPR in 2000, Bangladesh is bound to comply with the principles and standards articulated therein.

ARTICLE 19 OF THE ICCPR – FREEDOM OF EXPRESSION

Article 19 of the ICCPR guarantees the right of free expression "…regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media…" The United Nations (UN) Human Rights Committee, the implementing body of the ICCPR, has stated that, "any restrictions on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination systems" must comply with Article 19.[2]

Restrictions to the freedom of expression guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test.[3]

RESTRICTIONS ON FREEDOM OF EXPRESSION

Three-Part Cumulative Test

(1) the restriction must be provided by law, which is clear and accessible to everyone (i.e., adheres to principles of predictability and transparency);

(2) the restriction must pursue one of the purposes set out in article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; or (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and

(3) the restriction must be necessary and the least restrictive means required to achieve the purported aim (i.e., adhere to principles of necessity and proportionality).

The UN Human Rights Committee has stated that the burden lies with the State to show that any law or regulation restricting the freedom of expression passes Article 19's three-part test.[4]

2 Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 43, UN Doc # CCPR/C/GC/34 (2011).

3 See, e.g. United Nations Human Rights Council, A/HRC/17/27, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" May 16, 2011, para. 69.

4 Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 27, UN Doc # CCPR/C/GC/34 (2011).

While restrictions on the freedom of expression that fail the three-part test of Article 19 take many forms, two categories of such restrictions that feature prominently in the CSA are the over-regulation of online content and overbroad defamation laws; thus, the discussion of international legal standards here will focus on these types of restrictions.

REGULATION OF ONLINE CONTENT

The UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, in his report addressing the regulation of user-generated online content, has reiterated that States' duty to ensure freedom of expression includes the obligation to promote media diversity and independence, as well as access to information, and "…to ensure that private entities do not interfere with the freedoms of opinion and expression."[5] The Special Rapporteur in his report further flagged several specific issues with the approach to online content regulation taken by governments and private companies, including vague rules and policies around the promotion of terrorism,[6] as well as around hate speech, harassment, and abuse;[7] a lack of context when assessing the applicability of general restrictions;[8] automated flagging, removal, and filtering of content;[9] and a lack of notification or appropriate remedies where an appeal is granted.[10]

OVERBROAD DEFAMATION LAWS

Overbroad defamation laws, even if introduced for a legitimate purpose in accordance with Article 19(3) of the ICCPR, are likely to fail the first and third prongs of the three-part test. Defamation laws that are overbroad and vague in prohibiting permissible speech and/or in defining what may be constituted as defamatory would likely fail the first prong of the test; although such laws may accessible, they are likely to be unclear, in that people will not be able to ascertain what they can and cannot say to avoid violating the law. Such laws are also ripe for abuse and selective enforcement, and may encourage corruption, such as where the State protects the reputations of police, public officials and other powerful individuals with connections to the government.

Criminal defamation laws are likely to fail the third prong of the three-part test, as "imprisoning individuals for seeking, receiving and imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims un-

5 United Nations Human Rights Council, A/HRC/38/35, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye," April 6, 2018, para. 6.

6 Id. at para. 26.

7 Id. at para. 27.

8 Id. at para. 29.

9 Id. at para. 32.

10 Id. at para. 37-38.

der article 19, paragraph 3, of the [ICCPR],[11] and criminal penalties are not proportionate for harm to one's reputation caused by defamatory speech. Furthermore, criminal defamation laws fail the test of necessity, since defamation can and should be dealt with under civil laws as a matter between private actors, rather than as a matter of State prosecution.

ARTICLE 17 OF THE ICCPR - RIGHT TO PRIVACY

The right to privacy is enshrined in Article 17 of the ICCPR:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.[12] "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous."[13]

The special rapporteur for the freedom of expression has stated that the right to privacy should be subject to the same limitations test as the right to freedom of movement. The test provides: 1) the restriction must be provided by the law; 2) the essence of a human right is not subject to restrictions; 3) restrictions must be necessary in a democratic society; 4) any discretion exercised when implementing the restrictions must not be unfettered; 5) for a restriction to be permissible, it must be *necessary for the legitimate aim*; and 6) restrictive measures must conform to the principle of proportionality—appropri-

The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.

11 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 36, U.N. Doc. A/HRC/17/27 (16 May 2011); David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 33, UN Doc. # A/71/373, (September 2016); Ambeyi Ligabo, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paras. 39-43, UN Doc. A/HRC/7/14 (28 February 2008); Abid Hussain, Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion.

12 See Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, para. 4. 82 (Butterworth, 2004).

13 United Nations Human Rights Council, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," para. 23, A/HRC/23/40 (April 17, 2013).

ate to achieve protective function, least intrusive amongst those which might achieve the desired result, and proportionate to the interest to be protected.[14]

The freedom of expression and the right to privacy are interrelated: "The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression."[15] Just as a restriction to the freedom of expression must pass the three-part cumulative test derived from ICCPR Article 19 to be lawful, a restriction to the right to privacy is only lawful if it passes the test articulated above.

Under international law, investigation safeguards must exist to ensure that individuals' right to privacy is protected. Safeguards in the context of cybercrime legislation should include 1) requiring a warrant for any data collection or surveillance; 2) requiring a high judicial threshold; 3) limiting the scope of information collection to data related to alleged crimes; 4) setting limits in the duration of data collection or surveillance; 5) ensuring that private information and data is not shared beyond the scope of the investigation and either returned or deleted at the end of the judicial process.

14 Human Rights Committee, General Comment No. 27: Freedom of Movement (Article 12), para. 15, UN Doc. CCPR/C/21/Rev.1/Add.9 (1999); United Nations Human Rights Council, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," para. 29, A/HRC/23/40 (April 17, 2013).

15 United Nations Human Rights Council, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," para. 24, A/HRC/23/40(April 17, 2013).

3. Legal Framework for Internet and Digital Communications in Bangladesh

The CSA is the most recent law in a series of laws and policies introduced by the Government of Bangladesh to regulate online spaces. In 2002, the government adopted the National Information and Communication Technology Policy, which evolved into the "Digital Bangladesh" vision introduced in the 2008 election manifesto of the Awami League[16] for utilizing technology towards achieving development goals.

In 2006, the government adopted the Information Communication Technology Act ("ICT") and its implementing rules to address the legal recognition and security of information and communication technology and related matters. The ICT Act defines cybercrime as an offence.[17] As recently as 2023, activists and journalists have received sentences for violations under the ICT Act. The most prominent example was the sentencing of Adilur Raman Khan and ASM Nasiruddin Elan of the human rights NGO, Odhikar.

In 2014 the government released the National Cybersecurity Strategy of Bangladesh. The strategy aimed "to create a coherent vision for Bangladesh's information security in 2021, and highlights several national priorities to achieve this goal," including developing legislation, implementing protocols to reduce cyber vulnerabilities, and building capacity in cybersecurity. The integral component and the primary goal of the National Cybersecurity Strategy is the modernization of rules to prevent and prosecute cybercrimes on a priority basis.

THE DIGITAL SECURITY ACT

In 2018, the Digital Security Act 2018 (DSA) was enacted, supplanting the ICT Act as the foundation of the legislative framework relating to cybersecurity and cybercrimes. At the time, the government came to perceive the ICT Act as insufficient to address digital security and data protection concerns[18] and subsequently passed the DSA in 2018, superseding several sections of the ICT Act dealing with criminal offences related to online expression.

16 Dhaka Tribune. "Awami League manifesto: Surprise in IT." Dec. 18, 2018. Available at: https://archive.dhakatribune.com/bangladesh/election/2018/12/08/awami-league-manifesto-surprise-in-it.

17 Under the ICT Act, offences include: Section 54, the cognizable and non-bailable offence damage to computers, computer systems, and networks; Section 55, the offence of tampering with computer source code; Section 56, the offence of hacking a computer system; Section 57, the offence of publishing fake, obscene, or defaming information in electronic form and Section 66, the offence of using a computer for committing an offence. Section 57 of the ICT Act in particular, which brought within its scope the publication or dissemination of material "with a tendency to deprave or corrupt, deteriorate law and order, prejudice the image of the State, hurt religious belief, or instigate any person or organization," drew criticism for its suppression of free expression.

18 Page 48, Cybersecurity Capacity Review, Bangladesh, 2018, available at https://www.nrdcs.lt/file/repository/resources/CMM_Bangladesh_Report_FINAL.pdf.

In the years since its enactment, the DSA has been widely criticized for its violation of international standards relating to the freedom of expression, [19] the right to due process and in some cases, and the right to life.[20] The DSA has also been criticized for its inconsistencies with other Bangladeshi law and its application,[21] and the government's extensive use of the DSA against journalists and civil society activists.[22]

THE CYBER SECURITY ACT

In 2023, after widespread criticism of the DSA both domestically and internationally, the Government of Bangladesh decided to "transform" and "modernize" the controversial DSA through the new Cyber Security Act. Accordingly, the Government passed the Cyber Security Act (CSA) 2023 on September 13, 2023.

However, the CSA remains substantially similar to the controversial DSA and continues to criminalize various types of online speech. The CSA has retained most offenses under the DSA but makes ten offences bailable that were unbailable under the DSA. The new legislation continues to criminalize the freedom of expression, retains non-bailable offenses, and too easily could be misused to arrest, detain and silence critics.

In 2023, after widespread criticism of the DSA both domestically and internationally, the Government decided to "transform" and "modernize" the controversial DSA through the new Cyber Security Act. ... However, the CSA remains substantially similar to the DSA.

19 See e.g. Human Rights Watch, Bangladesh: Repeal Abusive Law Used in Crackdown on Critics, July 2020, https://www.hrw.org/news/2020/07/01/bangladesh-repeal-abusive-law-used-crackdown-critics.

20 United Nations Office of the High Commissioner for Human Rights. "Bangladesh: Bachelet urges review of Digital Security Act following death in custody of writer." March 1, 2021. Available at: https://www.ohchr.org/en/2021/03/bangladesh-bachelet-urges-review-digital-security-act-following-death-custody-writer.

21 https://www.thedailystar.net/law-our-rights/news/all-wrong-the-digital-security-act-2057321 and https://shuddhashar.com/law-review-digital-security-act-2018-and-questions-of-citizens-basic-human-rights/

22 See e.g. Human Rights Watch, Bangladesh: Repeal Abusive Law Used in Crackdown on Critics, July 2020, https://www.hrw.org/news/2020/07/01/bangladesh-repeal-abusive-law-used-crackdown-critics; United Nations Office of the High Commissioner for Human Rights. "Bangladesh: Bachelet urges review of Digital Security Act following death in custody of writer." March 1, 2021. Available at: https://www.ohchr.org/en/2021/03/bangladesh-bachelet-urges-review-digital-security-act-following-death-custody-writer.

4. Overview of the Cyber Security Act 2023

PURPOSE

The CSA was enacted to ensure "cyber security and for the identification, prevention, suppression, and trial of offences committed through digital or electronic means and matters ancillary thereto." Enacted as the replacement for the DSA, the CSA maintains similar purposes: to empower regulatory authorities to remove or block data or information, including through regulation of intermediary service providers, and to prosecute those who are in violation of its provisions regarding online activity.

SCOPE

The CSA addresses within its scope all publications, propagations and expressions for communication made in digital media or through digital process. It embraces all users, all electronic devices and systems, all equipment and outputs, and all personnel involved in digitalization, as well as illegal access to a computer/digital device/network.

Territorial Scope

Significantly, the CSA has extra-territorial application. As Section 4(1) of the Act states, "If any person commits any offense under this Act beyond Bangladesh which would be punishable offense under this Act if committed inside Bangladesh, then the provisions of this Act would be applicable in such manner if had those acts [been] committed in Bangladesh."

Additionally, the following extraterritorial provisions are also stipulated in the CSA:

- If any person commits an offence or contravention in Bangladesh under these provisions from outside Bangladesh using a computer, computer system, or computer network located in Bangladesh, then these provisions shall apply as if the entirety of the offence or contravention took place in Bangladesh (Section 4(2)); and
- If any person from within Bangladesh commits offence or contravention outside of Bangladesh under these provisions, then these provisions shall apply against them as if the entire process of the offence or contravention took place in Bangladesh (Section 4(3)).

Material Scope

The CSA covers all types of data processing including usage, saving and transmission, and all kinds of data, including critical information infrastructure, which may be designated as the government sees fit. In addition, the Act expressly covers certain types of personal data under the term 'identity information' (Section 26). Significantly, Section 37 of the CSA provides safe harbor protection for intermediaries, provided they can prove no knowledge and the exercise of due diligence, discussed further below.

Personal scope

The DSA applies to any natural person or institution, company, partnership business, farm or any other organization, and to any entity created by law, as well as to artificial legal entities. In the case of digital devices, the Act applies to its controller.

IMPLEMENTATION

The draft Cyber Security Rules 2024 (Rules) were shared with some civil society partners in May 2024. The discussions below on the Rules are based on the draft version. The stated objectives of the Rules are:

> i. To ensure the effective implementation of the Cyber Security Act, 2023;
>
> ii. To prevent, mitigate and respond to cyber security threats effectively, and to empower the Cyber Security Agency to provide a safer, more secure cyber environment; and
>
> iii. To protect critical information infrastructure.

The Rules are focused on the establishment of the Cyber Security Agency (Agency), the roles and responsibilities of the Agency, and on identifying and protecting critical information infrastructure under Section 58 of the CSA.

Section 58 of the CSA states that:

> (1) The Government may, by notification in the official Gazette, make rules for carrying out the purposes of this Act.
>
> (2) Without prejudice to the generality of sub-section (1), the Government may, *inter alia*, make rules especially for all or any of the following matters, by notification in the official Gazette, namely:
>
> (a) establishment of digital forensic lab;
>
> (b) supervision of digital forensic lab by the Director General;
>
> (c) review of traffic data or information and the process of its collection and preservation;
>
> (d) process of interference, review or decryption and protection;
>
> (e) security of critical information infrastructure;
>
> (f) procedure of regional and international cooperation in case of cyber security;
>
> (g) formation and operation of Emergency Response Team and coordination with other teams;
>
> (h) cloud computing, metadata; and
>
> (i) protection of preserved data.

National Cyber Security Agency

Composition

The National Cyber Security Agency ("Agency") consists of one Director General ("DG") and five Directors, who are appointed as full-time employees by the government. In addition, the Agency can appoint a significant number of employees.

As per section 6 of the CSA, "The Director will be a specialist / expert on computer or cyber security, he will be appointed by the Government and terms of employment will be determined by the Government." Reference to the "Government" here refers to the Information and Communication Technology Division (ICT Division) under the Ministry of Posts, Telecommunication and Information Technology. The appointment and removal power of the Government, through the ICT Division, is not guided by objective standards; rather, appointment and removal could come at any time and for any reason. Consequently, the DG of the Agency is not fully independent.

The DG is solely responsible for staff recruitment and the operation and administration of the Agency. The DG is responsible for determining the appropriate response to digital security threats and incidents, based on the level of severity.

Powers, Duties, and Responsibilities

The Agency is authorized to identify and designate "Critical Information Infrastructure" both in government and other relevant sectors; the Agency is to develop plans and strategies for the protection of such information systems.

The Agency is authorized to enter, inspect, search, examine or suggest security measures, request compliance reports, and conduct digital security audits of designated infrastructure (as per Section 16 of CSA). The Agency has the power to take action if digital security is under threat in terms of national security, foreign relations, public health, public order or providing necessary or essential service. An essential service means any service essential to the national security, defense, foreign relations, economy, public health, public safety or public order of Bangladesh.

"The National Cyber Security Agency is authorized to identify and designate "Critical Information Infrastructure" both in government and other relevant sectors; the Agency is to develop plans and strategies for the protection of such information systems.

The powers, duties, and responsibilities of the Agency include:

1. Coordination and Instruction: Coordinate with relevant governmental and non-governmental organizations during IT-related state crises, providing necessary instructions for resolution.
2. Policy and Standards Formulation: Develop guidelines, policies, strategies, and standards for auditing critical information infrastructure, forensic labs, and IT systems.
3. Critical Information Infrastructure Security:
    - Ensure the safety of critical information infrastructure through necessary measures and inspections.
    - Develop and monitor procedures to reduce risks and enhance safety.
    - Formulate and enforce operating procedures and maintenance criteria for individuals involved in such infrastructure.
4. Digital Forensic Labs: Establish, manage, maintain, and control digital forensic laboratories.
5. Quality Assurance: Determine the quality standards for computer hardware, software, services, and products used in cyber security.
6. Competency and Capacity Building: Set competency standards for cyber security personnel and enhance capacity in computer and system security oversight.
7. Cyber Security Services: Introduce, operate, maintain, monitor, and control cyber security services while fostering cooperation among service providers.
8. Research and Development: Undertake research activities related to cyber security and support its development.
9. Sectoral IT Security: Ensure the security of information and communication technology across various sectors, including universities and research institutions.
10. Standards Compliance: Monitor compliance with prescribed cyber security standards.
11. Threat Monitoring and Response: Monitor domestic and international cyber security threats, alert relevant parties, and take remedial measures.
12. Proactive Threat Prevention: Implement proactive measures to prevent cyber security threats impacting national security, foreign affairs, public health, public order, or essential services.
13. International Cooperation: Engage in mutual cooperation with foreign authorities regarding cyber security incidents and represent the government in international forums.

14. Industry Development: Promote the expansion and development of the cyber security industry and assist in improving the skills and professional standards of industry personnel.
15. Information Collection and Recommendations: Collect and review cyber security-related information from domestic and international sources, making recommendations to the government.
16. Public Awareness and Training: Conduct public awareness activities, including organizing training, workshops, and seminars on cyber security.
17. Investigation and Remediation: Investigate vulnerabilities, breaches, and malicious activities in cyber security systems.
18. International Collaboration: Execute memorandums of understanding, agreements, and cooperation with international organizations and foreign governments.
19. Advisory Role: Advise the government on national cyber security policy matters.

National Cyber Security Council

Composition

The Chair of the National Cyber Security Council ("Council") is the Prime Minister, and the other 15 Council members include representatives from various ministries.

Powers, Duties, and Responsibilities

As per Section 13 of the CSA, the powers, duties, and responsibilities of the Council include:

- providing necessary directions on how to remedy a situation where cyber security is under threat;
- advising on how to improve the cyber security infrastructure, how to increase its manpower, and how to increase its quality;
- enacting inter-institutional policies to ensure cyber security;
- taking necessary steps to ensure the implementation of the Cyber Security Act and of the Rules enacted under the Cyber Security Act;
- directing the Agency to establish more forensic labs; and
- approving emergency meeting requests by the Director General of the National Cyber Security Agency in the event of a cyber security threat or threat to critical information infrastructure.

Digital Forensic Lab

Powers, Duties, and Responsibilities

The National Cyber Security Agency is responsible for the control and supervision of digital forensic labs under the CSA, with rules prescribing the establishment, use, operation and other matters of the digital forensic labs.[23] The digital forensic labs are responsible for conducting forensic analysis on digital evidence and providing expert opinions, including evidence as expert witnesses in court.

All cyber-crimes, as defined under the Code of Criminal Procedure Act V of 1898, are investigated in the forensic lab. Neither the Act nor the draft Rules, however, establish a standardized approach to ensure consistent handling of all cases identified as "threats to cyber security." There are no procedures for ensuring accountability, maintaining a database of such actions, or disclosing these actions to the public. The only exception is the requirement to publish communications with the National Computer Emergency Response Team on the agency's website, as mandated by section 8 of the Rules.

National Computer Emergency Response Team

Composition

The National Computer Emergency Response Team (NCERT) shall consist of persons specializing in cyber security and if necessary, members of law enforcement agencies. Section 9(4) of the CSA states that the NCERT shall be on duty full time, in the manner prescribed by the implementing rules.

Powers, Duties, and Responsibilities

Section 9(5) of the CSA outlines the functions of the NCERT, namely:

- ensuring the emergency security of critical information infrastructure;
- taking immediate action for remedy if there is any cyber or digital attack or if the cyber or digital security is affected;
- taking necessary steps to prevent probable and imminent cyber or digital attacks;
- carrying out all co-operative activities, including the exchange of information with a similar foreign team or organization, with the approval of the Government, for this Act; and
- other functions prescribed by the implementing rules.

23 Digital Security Act, Section 10.

5. Key Provisions of the Cyber Security Act 2023 and Assessment Under International Standards

POSITIVE OBLIGATIONS

Designation of "critical information infrastructure"

The CSA[24] defines "critical information infrastructure" ("CII") as "…any external or virtual information infrastructure declared by the government that controls, processes, circulates or preserves 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 [or] (ii) national security or national integrity or sovereignty."[25]

The CSA goes on to articulate that in order "To fulfill the objective of this Act, the Government may, by notification in the official Gazette, declare any computer system, network or Information Infrastructure as critical information infrastructure."[26]

COMPLIANCE:

Critical Infrastructure Requirements

Once a system – even if privately owned and operated – is declared to be critical infrastructure, the owner must submit annual inspection reports to the government and follow certain rules, including using Agency-approved networks and products, making Agency-approved purchases of goods, seeking consent before transferring data outside the country, and undergoing mandatory security testing.[27]

Owners of computers designated as CII are subject to various statutory duties, which include notifying the Agency of a change in ownership and undergoing digital security audits and digital security risk assessments. Non-compliance with the statutory duties without reasonable justification is a criminal offence punishable by fine and/or imprisonment.

24 The analysis of the CSA in this handbook is based on translation provided by the International Center for Not-for-Profit Law (ICNL) of the enacted law. We understand that the government has used ICNL's translated version as the English version.

25 CSA, Section 2(g).

26 CSA, Section 15.

27 CSA, Section 16(2) and CSA Rules, Section 16.

How does this provision measure up to international standards?

These are broad, vague powers, without adequate oversight or safeguards. The definition of CII is overbroad and allows for the designation as CII of anything "adversely affecting" public safety, public health, national security etc., which gives the government wide discretion and invites abuse, such as if the government targets the infrastructure of human rights activists or religious minorities, and on this basis conducts ongoing monitoring and inspection of the CII in question (as allowed by Section 16 of the Act).

Obligation of service providers

The CSA defines a "service provider" as "any person who enables any user to communicate through computer or digital process; or any person, entity or institution who or which processes or preserves computer data in favour of the service or the user of the service."[28]

According to Section 37 of the CSA, "No service provider shall be liable under this Act or rules made thereunder for facilitating access to any data-information, if he proves that the offence or breach was committed without his knowledge or he exercised all due diligence to prevent the offence."

Section 37 essentially imposes a positive obligation on service providers, protecting service providers from liability as long as they can prove that they were "not aware of the offence or tried their best to prevent the commission of the offence."

How does this provision measure up to international standards?

Under international standards, such as the Manila Principles on Intermediary Liability, intermediary providers should be shielded from liability for third-party content. The obligation imposed on service providers under Section 37 is overbroad, encompassing any content posted on their platforms, and is likely to lead to the removal of content whenever someone claims the content breaches the law. This is due to the fact that service providers will not be able to verify all of the claims and so will simply take the content down rather than risk taking on liability. Therefore, this provision will likely result in the removal of legitimate content and violate the freedom of expression.

28 Digital Security Act, Section 2(w)

COMPUTER/DIGITAL/ELECTRONIC-RELATED OFFENCES

Chapter VI of the CSA retains 17 of the 18 offences created under the DSA and articulates the applicable punishment for each of these. The Act also stipulates that anyone abetting the commitment of an offence under the Act shall be deemed to have committed an offence and is subject to the same punishment that is provided for by the offence.[29]

Of Chapter VI's 17 offences, 11 of these offences relate to actions committed in the digital space—*irrespective of the substantive content involved in the action,* with the exception of identity fraud-related offences, which necessarily relate to the content involved—using a digital or electronic medium or involving illegal access or destruction of CII or computers/computer systems. The remaining offences relate to the substantive content in question.

The following chart outlines the 11 offences relating to actions committed in the digital space where the specific content involved is not relevant to the offence, while the other offences established under the Act are articulated later in this section.

Section & Conduct Prohibited	Punishment
17. Illegal access to critical information infrastructure • Illegal access to any CII • Causing or trying to cause harm or damage to CII by means of illegal access	• Imprisonment up to 3 years and/or fine up to Taka 25 lac[30] • Imprisonment up to 6 years and/or fine up to Taka 1 crore[31]
18. Illegal access to computer, digital device, computer system • Making or abetting illegal access to any computer/computer system/computer network • Making or abetting illegal access with intent to commit an offence	• Imprisonment up to 6 months and/or fine up to Taka 2 lac • Imprisonment up to 3 years and/or fine up to Taka 10 lac
19. Damage of computer, computer system • Collecting any data, data-storage, information or any extract of it from any computer, computer system/computer network • Intentionally inserting/ trying to insert any virus or malware or harmful software into any computer/computer system/computer network • Willingly causing or trying to cause harm to data or data-storage of any computer/computer system/computer network • Obstructing or trying to obstruct a valid or authorized person to access any computer/computer system/computer network • Willingly creating or selling, or trying to create or sell spam or send unsolicited electronic mail without permission of the sender or receiver, for marketing any product or service • Taking service of any person, or depositing or trying to credit the charge fixed for the service to the account of any other person fraudulently or by means of unfair interference	• Imprisonment up to 7 years and/or fine up to Taka 10 lac

29 Section 33 of the CSA

30 "Lac" refers to a unit of measure equal to one hundred thousand (100,000). 25 lac is the equivalent of 2,5000,000 rupees.

31 "Crore" refers to a unit of measure equal to ten million (10,000,000).

Section & Conduct Prohibited	Punishment
20. Modification of computer source code • Intentionally or knowingly hiding, damaging, or modifying the source code used in any computer programme/computer system/computer network, or trying to through another person, and if such source code is preservable or maintainable	• Imprisonment up to 3 years and/or fine up to Taka 3 lac
22. Digital or electronic forgery • Committing forgery by using any digital or electronic medium	• Imprisonment up to 2 years and/or fine up to Taka 5 lac
23. Digital or electronic fraud • Committing fraud by using any digital or electronic medium	• Imprisonment up to 5 years and/or fine up to Taka 5 lac
24. Identity fraud or personation • Intentionally or knowingly using any computer/computer programme/computer system/computer network/digital device/digital system/digital network while holding the identity of another person or exhibiting the personal information of another person as his own in order to deceive or cheat • Holding the personal identity of any person, alive or dead, as his own in order to gain benefit for himself or another person, acquire any property or interest therein or cause harm to a person by impersonating someone	• Imprisonment up to 5 years and/or fine up to Taka 5 lac
26. Unauthorized collection/use of identity information • Collecting, selling, possessing, providing or using identity information of any other person without lawful authority	• Imprisonment up to 2 years and/or fine up to Taka 5 lac
27. Cyber terrorism • Obstructing legal access to, or illegally accessing any computer/computer network/ internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or creating pollution or inserting malware in any digital device which may cause or is likely to cause death or serious injury to a person; or affecting or damaging the supply and service of daily commodity of public or creating adverse effect on any critical information infrastructure; or intentionally or knowingly gaining access to, or making interference with, any computer/computer network/internet network/protected data-information/computer database or gaining access to any such protected data information or computer database which may be used against friendly relations with another foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group	• Imprisonment up to 14 years and/or fine up to Taka 1 crore
30. E-transaction without legal authority • Making, without legal authority, e-transaction over electronic and digital means from any bank, insurance or any other financial institution or any organisation providing mobile money service; or making any e-transaction though the e-transaction is, from time to time, declared illegal by the Government or Bangladesh Bank	• Fine not exceeding Taka 25 lac
32. Hacking • Stealing, destroying, cancelling or changing any information of the computer data storage, or reducing the value or efficacy of it or causing harm in any way; or • Causing harm to any computer, server, computer network or any other electronic system	• Imprisonment up to 14 years and/or fine up to Taka 1 crore

How do these provisions measure up to international standards?

Section 27 uses vague terms to define "cyberterrorism" while it envisions severe penalties. The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recommends that "terrorist offences" should be confined to instances where the following three conditions cumulatively meet: (a) acts committed with the intention of causing death or serious bodily injury, or the taking of hostages; (b) for the purpose of provoking a state of terror, intimidating a population, or compelling a government or international organization to do or abstain from doing any act; and (c) constituting offences within the scope of and as defined in the international conventions and protocols relating to terrorism. Similarly, any criminalization of conduct in support of terrorist offences should be restricted to conduct in support of offences having all these characteristics."[32] Section 27 is at risk, through arbitrary enforcement, of being used to target human rights defenders, journalists, and whistleblowers.

Similarly, Section 32 criminalizes hacking and defines it to include action that is intended to "cause harm in any way," inviting arbitrary interpretation and application. A narrower definition would be more appropriate, such as requiring intent to cause "injury or serious harm."[33]

The lack of precision in these provisions thus leaves significant discretion for enforcement with the authorities, creating the potential for abuse and violations of individuals' fundamental rights, including due process.

32 United Nations Commission on Human Rights, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, para. 72 E/CN.4/2006/98 (2005).

33 The Budapest Convention on Cybercrime, the only major treaty addressing cybercrimes, includes provisions requiring states to criminalize illegal access, illegal interception, and data and system interference. However, these provisions require the act to be "committed intentionally." For example, to qualify as illegal access, the access to the computer system must be without right and occur "with the intent of obtaining computer data or other dishonest intent." Bangladesh has not yet signed the Convention and the Convention. However, the standards set forth in the Convention represent an emerging minimum consensus, including among the 75 States that have signed or ratified the treaty. For a list of signatories and ratifications, please see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=DOzYeqZn.

CONTENT RESTRICTIONS

Offensive or Hostile Speech:

Three provisions under the CSA target inflammatory or hostile speech.

Section & Conduct Prohibited	Punishment
21. Carrying out any hateful, confusing and defamatory campaign about liberation war, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag • Making or instigating, by means of digital medium, any hateful or confusing and defamatory campaign about the liberation war of Bangladesh, spirit of liberation war, father of the nation, national anthem or national flag	• Imprisonment up to 5 years and/or fine up to Taka 1 crore or both
28. Publication, broadcast of information in website or in any electronic format that hurts religious values or sentiment • Willingly or knowingly publishing or broadcasting, or causing to publish or broadcast, anything on website or in any electronic format, which hurts religious sentiment or values, with an intention to hurt or provoke religious values or sentiments	• Imprisonment up to 2 years and/or fine up to Taka 5 lac
31. Deteriorating law and order • Intentionally publishing or transmitting anything on website or in digital layout that creates enmity, hatred or hostility among different classes or communities of society, or destroys communal harmony, or creates unrest or disorder, or deteriorates or undermines public order	• Imprisonment up to 5 years and/or fine up to Taka 25 lacs

How do these provisions measure up to international standards?

These three sections are overbroad and vague, and do not meet the standard under international law for restricting hate speech, which must also comply with Article 19's three-part test of legality, legitimacy, and proportionality. Consequently, implementation of these provisions is likely to result in violations of freedom of expression. What would constitute speech "against" the liberation war (Section 21)? What speech "hurts religious values or sentiments" (Section 28), or "deteriorates law and order" (Section 31)? These provisions are not clear; those communicating online are unable to predict how these provisions will be applied. These provisions could be applied against expression and dissent. Violation of these provisions could also result in imprisonment and heavy fines, which do not constitute necessary or the least restrictive means of achieving the purported aims. Section 31 is also likely to unduly restrict freedom of association protected under Article 22 of the ICCPR.

False Information:

Two sections of the CSA criminalize the publication of information that is "false."

Section & Conduct Prohibited	Punishment
25. Transmission, publication of offensive, false or threatening data information • Intentionally or knowingly transmitting, publishing or propagating, through any website or any other digital medium, any data-information which the person knows to be offensive, false or threatening, in order to annoy, insult, humiliate or malign a person OR publishing or propagating or abetting others to publish or propagate any information, as a whole or partly, which the person knows to be propaganda or false, with an intention to affect the image or reputation of the country, or to spread confusion	• Imprisonment up to 2 years and/or fine not exceeding Taka 3 lac or with both
29. Publication, transmission, etc. of defamatory information • Publishing or transmitting any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) on website or in any other electronic format	• Fine not exceeding Taka 25 lacs

How do these provisions measure up to international standards?

These provisions are overly broad and vague and would likely restrict permissible speech from being published. Prohibiting "false" or "fake" information is incompatible with the freedom of expression.[34] Rather than prevent the spread of misinformation or disinformation,[35] laws that prohibit "false" content often chill the dissemination of legitimate and important expression to the public.

Section 25 also criminalizes "offensive" speech, which is protected under international law. Restrictions against speech that "annoy, insult, humiliate, or malign" are particularly disfavored under international human rights law. The ICCPR does not make exceptions to protect "ideas or beliefs from ridicule, abuse, criticism, or other 'attacks' seen as offensive."[36]

In addition, these provisions effectively criminalize defamation. Defamation laws that are overbroad and vague in prohibiting permissible speech and/or in defining what may be constituted as defamatory are likely to be unclear, in that people will not be able to

34 See, The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on "Fake News", Disinformation and Propaganda, para. 2(a) (March 3, 2017).

35 According to UNESCO, 'misinformation' is defined as "[i]nformation that is false but not created with the intention of causing harm," while 'disinformation' is "[i]nformation that is false and deliberately created to harm a person, social group, organisation or country." (Mal-information is "[i]nformation that is based on reality, used to inflict harm on a person, social group, organisation or country.") Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training, UNESCO, https://en.unesco.org/fightfakenews.

36 UN General Assembly, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," para. 21, UN Doc. A/74/486 (9 October 2019).

(continued)

ascertain what they can and cannot say to avoid violating the law. Such laws are also ripe for abuse and selective enforcement, and may encourage corruption, such as where the State protects the reputations of police, public officials and other powerful individuals with connections to the government.

The Special Rapporteur on the promotion and protection of the right to freedom of expression has called on all States to decriminalize defamation.[37] As the Special Rapporteur has elaborated, criminal defamation laws are likely to fail the third prong of the three-part test, as "imprisoning individuals for seeking, receiving and imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under article 19, paragraph 3, of the [ICCPR],"[38] and criminal penalties are not proportionate for harm to one's reputation caused by defamatory speech. Furthermore, criminal defamation laws fail the test of necessity, since defamation can and should be dealt with under civil laws as a matter between private actors, rather than as a matter of State prosecution.

STATE POWERS

The CSA grants the government extensive powers to facilitate various provisions of the Act.

Power to remove or block data

Section 8 of the CSA gives the Director General of the Cyber Security Agency the authority to request the Bangladesh Telecommunications and Regulatory Commission (BTRC) to remove or block data-information that "creates threat to digital security" or "hampers the solidarity, financial activities, security, defence, religious values or public discipline of the country or any part thereof, or incites racial hostility and hatred."

It is important to note that there are neither specific criteria nor prescribed procedures outlined in the Act or the draft Rules for executing such actions. There appears to be no judicial oversight of these decisions, nor a process for individuals or entities to challenge the decision to block or remove data-information. The discretion to make these decisions appears to rest solely with the Director General.

37 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 73, U.N. Doc. A/HRC/17/27 (16 May 2011).

38 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 36, U.N. Doc. A/HRC/17/27 (16 May 2011); David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 33, UN Doc. # A/71/373, (September 2016); Ambeyi Ligabo, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paras. 39-43, UN Doc. A/HRC/7/14 (28 February 2008); Abid Hussain, Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion.

How does this provision measure up to international standards?

Section 8 is far too broad and would result in the censorship of legitimate expression in violation of international law. It is unclear what data-information could be considered to threaten digital security or to hamper solidarity, religious values, etc. and, as such, any publishers of content may find themselves coming under the purview of the Act and having their content blocked or removed. For example, under the Act, if an individual publishes a social media post criticizing organized religion, this could be deemed as hampering religious values and could thus be subject to removal. Such categories of expression are protected under the right to freedom of expression, which includes expression that offends, shocks or disturbs.[39]

Monitoring of critical information infrastructure

Along with imposing obligations on owners of infrastructure that has been designated as CII, the CSA also grants powers to the government to monitor and inspect infrastructure that has been declared as CII. Under Section 16 of the Act, the government is entitled to receive an inspection report of CII every year, and under Section 16(3) "if the Director General has reason to believe that any activity of an individual regarding any matter within his jurisdiction is threatening or detrimental to any critical information infrastructure, then he may, *suo moto*, or upon a complaint of any other person, inquire into the matter."

How does this provision measure up to international standards?

In conjunction with the vague and overbroad definition of CII, this provision allows for the monitoring and inspection of anything "adversely affecting" public safety, public health, national security etc., which gives the government broad discretion and invites government overreach. For example, the government could target the infrastructure of human rights activists or religious minorities, and on this basis conduct ongoing monitoring and inspection of the CII in question. As a result, there is significant potential for interference with the freedom of expression.

39 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 37, UN Doc. # A/HRC/17/27 (May 2011).

Investigation powers

Section 40 of the CSA grants significant powers to the Investigation Officer within the scope of an investigation under the Act, including to take any computer/computer infrastructure into custody, "collecting data-information of traffic data from any person or agency;" and taking other steps as necessary.

How does this provision measure up to international standards?

In conjunction with the other provisions of the CSA, including the definition of CII and the vague and overbroad content prohibitions outlined above, the investigation powers granted by Section 40 are overbroad and could be susceptible to abuses resulting in violations of the freedom of expression and a general chilling effect.

Search and seizure

Section 41 of the CSA allows for search and seizure by warrant, stating that, "If a police officer has reasons to believe that (a) any offence has been committed or is likely to be committed under this Act; or (b) any computer, computer system, computer network, data information related to an offence committed under this Act, or any evidence thereof has been preserved in any place or to a person, then he may, for reasons of such belief to be recorded in writing, obtain a search warrant upon an application to the Tribunal or the Chief Judicial Magistrate or the Chief Metropolitan Magistrate." In this situation, the police officer may take the following measures: "taking possession of the data-information of traffic data under the possession of any service provider," or "creating obstruction, at any stage of communication, to any telegraph or electronic communication including recipient information and data-information of traffic data."

Section 42 of the Act goes on to articulate the circumstances under which a police officer has the authority to carry out a search, seizure, and arrest without a warrant. A warrant is not needed when "... a police officer has reasons to believe that an offence under this Act has been or is being committed, or is likely to be committed in any place, or any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way." In this situation, a police officer may take the following measures: "(a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure; (b) to seize the computer, computer system, computer network, data information or other materials used in committing the offence or any document supportive to prove the offence; (c) to search the body of any person present in the place; (d) to arrest any person present in the place if the person is suspected to have committed or be committing an offence under this Act."

How does this provision measure up to international standards?

The provisions for search and seizure both with and without warrants are problematic particularly in the context of the various provisions highlighted above. The threshold for granting a warrant is quite low and contains no mention of how the data-information collected will be treated, opening the door for broad and unlimited surveillance. For example, if a police officer has reason to believe that an offence has been or is likely to be committed under the Act (including the vague and overbroad offenses articulated above), they have broad powers of search and seizure and can go on 'fishing expedition'. These provisions are ripe for abuse and could enable the targeting of activists and minority groups. As such, they are likely to have a significant chilling effect on the freedom of expression, as well as on the freedom of association and other related rights.

6. Implementation of the Cyber Security Act 2023

Since the CSA was adopted and implemented in 2023, cases have already been brought against individuals for online expression criminalized under the law. For example, the authorities arrested one man under the CSA after he criticized the quota system for government jobs in June 2024 on Facebook.[40] In February 2024, activist Shamim Ashraf was arrested under the CSA for designing posters that criticized the city of Mymensingh, in a case filed by the city corporation.[41] In December 2023, four journalists were sued under the CSA for news articles they published regarding another journalist's marital affair, under the charge that the information was published with the intention to humiliate him, a criminal penalty under Section 25 of the CSA.[42]

Because the CSA is substantially similar to the DSA, it is likely that the CSA will be implemented in the same widespread and punitive manner that the DSA was, suppressing online expression and dissent. Examples of criminal cases brought under the DSA remain relevant for forecasting how the CSA will be implemented in the coming months and years.

The Centre for Governance Studies (CGS), which tracks cases brought under the DSA, has recorded 1,436 cases brought under the DSA between October 8, 2018 and June 25, 2024.[43] Based on the Centre's data analysis, the highest number of cases monitored were brought under Section 25 (269 cases), publication of information with intention to humiliate/insult, and Section 29 (268 cases), defamation. Both provisions have been retained by the CSA, although the jail sentence associated with Section 29 has been removed.

Section 25 was used widely against online social media users and journalists. For example, during 2020, at the height of the COVID pandemic, two dozen people were arrested for critical

Because the CSA is substantially similar to the DSA, it is likely that the CSA will be implemented in the same widespread and punitive manner that the DSA was, suppressing online expression and dissent.

40 https://www.thedailystar.net/news/bangladesh/crime-justice/news/cyber-security-act-man-sent-jail-over-fb-post-3637876

41 https://www.observerbd.com/news.php?id=461000

42 https://www.thedailystar.net/news/bangladesh/news/four-journalists-sued-under-csa-3649281

43 https://freedominfo.net/

online expression about coronavirus.[44] In the year 2020 alone, over 100 people were sued for expressing their opinions on Facebook and other social media platforms.

Under the DSA, minors were also arrested and charged with violations. For example, a 9th grade student was arrested in June 2020 for posting on social media content that allegedly "defamed" then-Prime Minister Sheikh Hasina, despite the teenager later deleting the post and posting an apology.[45] In this instance, the case was filed by a local Juba League leader, and not the police. According to CGS's data, 47.9% of the plaintiffs in DSA cases are individuals.

Another provision used frequently under the DSA was Section 31 (168 cases recorded by CGS), often against journalists, for online expression that "creates enmity, hatred, hostility among different classes … or destroys communal harmony." Section 31 is retained in the CSA and is likely to be used in a similar way against journalists.

With no clear definition of what speech would be considered a violation of the law, the provision leaves the government wide scope to prosecute speech it does not like. Moreover, almost any criticism of the government may lead to dissatisfaction and the possibility of public protests. For example, the CSA was used in connection with the widespread protests in late July 2024 in response to the government jobs quota system, including against seven individuals who were arrested and charged for publishing "satirical pictures and taunting government officials" on Facebook.[46]

44 https://www.newagebd.net/article/105935/8-journalists-held-in-a-week-under-digital-security-act

45 https://www.dhakatribune.com/bangladesh/nation/213828/9th-grader-arrested-in-dsa-case-accused-of

46 https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/

7. Conclusion

Although the Cyber Security Act, 2023 was enacted with the purpose of improving the controversial Digital Security Act, 2018, an assessment of the provisions of the Act suggests that many of the same concerns remain and that the CSA poses continued risk to fundamental civic freedoms. Many provisions of the CSA fail to meet the standards set out in international law and invite continuing government interference in the freedom of expression. It remains an open question as to whether the new interim government will refrain from the restrictive implementation of the CSA and/or call for the repeal or revision of the CSA.

USAID
FROM THE AMERICAN PEOPLE

COUNTERPART
INTERNATIONAL
In partnership for
results that last.

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

1660 L Street NW, Suite 600, Washington, DC 20036 USA
www.icnl.org | facebook.com/ICNLAlliance | twitter.com/ICNLAlliance