Recommendations on Cyber Shurokkha Ordinance 2024 from BLAST

1. The Bangladesh Legal Aid and Services Trust (BLAST) has prepared this submission on the draft 'Cyber Protection Ordinance 2024' (CSO).
2. BLAST welcomes the decision to repeal the Cyber Security Act 2023 (CSA), in recognition of the need to address the concerns raised about its application, including the removal of most speech offences and the omission of pending cases related to these offences through the saving clause in the draft. BLAST also welcomes the Government's move to address harmful content instead of penalising speech based on sentiments and reputation.
3. However, BLAST is concerned regarding the proposed ordinance's introduction of offences with some adopted from the colonial era laws and the newer abusive laws, retention of provisions providing unfettered powers to the various authorities including for blocking content, lack of sufficient safeguards for individuals accused or arrested under the proposed law, and continuing ambiguity with regards to the procedures to be followed for trials and appeals.
4. In this context, BLAST respectfully submits that the Government hold open consultations with all concerned stakeholders, and in particular with women's groups, child rights' groups, development organisations, representatives of marginalised communities, disabled people's organisations, technology law experts, and technology experts.
5. BLAST has conducted consultations with representatives of organisations focusing on women's and children's rights, including those addressing online harassment, as well as with research experts and practitioners in technology law, to gather input on this submission. Addressing the following key areas is crucial to ensure clarity, prevent inconsistent enforcement, and protect fundamental freedoms and rights:

KEY CONCERNS AND RECOMMENDATIONS

Harmful Content		
Section	**Review and Comments**	**Recommendations**
25	Penalises the intentional dissemination or threat to dissemination of information, obscene videos, audio visuals, still images, captured through graphics or other means, editable, produced through Artificial Intelligence, or editable or displayable data-information which is harmful or intimidating and used to blackmail through sexual harassment or revenge porn. "Blackmailing" is defined as a threat or intimidation to publish private information or cause harm to coerce an individual into granting illegal advantages or services. The definition of blackmail remains ambiguous, without clarity on the	a. Separately penalise the offenses of 'sexual harassment' and 'revenge porn' due to their distinct levels of impact and harm. Define these terms precisely to prevent overlap, acknowledging that each may include the other despite distinct consequences. Take guidance from definitions from other jurisdictions, working definitions developed by UN entities, and the Global Partnership for Action. Exclude blackmail to prevent overlap with 'sexual harassment' and 'revenge porn'. b. Define "Online Sexual Harassment" as technology-facilitated unwelcome sexual

	parameters of "harmful or intimidating" and what constitutes "private information". The draft also fails to define the terms "sexual harassment" and "revenge porn". These gaps provide a scope for subjective interpretation of the content deemed harmful and inconsistent application of the proposed ordinance. The criminalisation of videos deemed "obscene" remains a significant legal challenge, rooted in the subjective moral and cultural values of the colonial-era Penal Code, 1860. This subjectivity risks hindering freedom of expression including through disproportionately affecting women and contributing to a culture of self-censorship among content creators, artists, and individuals. The broadness of this term complicates enforcement and allows for inconsistent application. Obscenity laws are often misused, including against women under the Pornography Control Act 2012 (PCA), leading to instances of moral policing. If the draft Ordinance is promulgated, there would be a scope for multiplicity of proceedings for the same action under the Penal Code, PCA, and the CSO as all address 'obscenity' without distinct jurisdictional boundaries.	advances, requests for sexual favours, conduct or gestures of a sexual nature, or any other behaviour of a sexual nature. This may include repeated requests for nude images or acts such as cyberflashing, sextortion, or revenge porn.[1] c. Define "Cyberflashing" as a form of image-based abuse involving the unsolicited sending of images of a person's genitals or sexually explicit materials. This includes unsolicited pornography, violent rape porn gifs, or altered photographs where the target's image has been sexualised.[2] d. Define "sextortion" as the act where an individual possesses or claims to possess a sexual image or video of another person and uses it to coerce or extort actions from the individual against their will.[3] e. Define "revenge porn" as the non-consensual sharing of intimate images or videos, including the exemptions by reflecting Section 188 of the UK's Online Safety Act 2023 amending the UK's Sexual Offences Act 2003. f. The term "obscene material" should be excluded to prevent its misuse. g. Provide clear legal standards or thresholds for content to be deemed harmful, and remove the word intimidating to avoid arbitrary enforcement. h. Amend the Pornography Control Act, 2012 through the CSO to criminalise digital child sexual abuse material, and digital non-consensual pornography, and incorporate the definitions of digital pornography, digital child sexual abuse material, and digital non-consensual pornography as

[1] The definition is a combination of UNICEF's definition of sexual harassment, Australia's e-Safety Commissioner's guidelines on online sexual harassment, and Global Partnership for Action on Gender-Based Online Harassment and Abuse's resources with analysis by the United Nations Population Fund (UNFPA) and Australia's eSafety Commissioner on behalf of the Global Partnership for Action on Gender-Based Online Harassment and Abuse (Global Partnership).

[2] Global Partnership for Action on Gender-Based Online Harassment and Abuse

[3] ibid.

		follows to ensure precision, consistency in application of the laws, and address online harm adequately. • "digital pornography" means any material, in any medium, created using any digital or electronic medium that expressly and predominantly depicts or describes, of or related to a person, any real or simulated sexually explicit acts, or any sexually explicit communication, or any sexual organs, or any sexual exploitation or abuse, or any sexual services, which lacks significant literary, research, artistic, political, cultural, historical, religious, educational, media reporting, law enforcement and criminal investigation, medical, or scientific value or purpose, and it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification, but excludes child sexual abuse material, non-consensual pornography, or technology-facilitated sexual violence; provided that the term "create" and its variants shall include, without limitation, the act of generating, modifying, manipulating, synthesizing, superimposing, or otherwise altering any digital or visual material or representation to resemble or depict a real person, regardless of whether such likeness was originally derived from a real image or generated entirely through digital means. **"digital child sexual abuse material" means any material or representation, in any medium, created using any digital or electronic medium that:** (a) visually, audibly, or textually, or otherwise, depicts or describes: (i) any real or simulated sexually explicit acts, or (ii) any sexual organs, or (iii) sexual exploitation or abuse, or sexual services, (iv) sexually explicit communication with another person, including a child, or (v) sex offenses as defined under the

		applicable laws, of, or related to, or in the presence of, any child (as defined in sections 2(17) and 4 of the Children Act, 2013 (Act No. XXIV of 2013), or (b) visually, audibly, or textually, or otherwise, causes, incites, encourages, or instructs any child to: (i) engage in, or observe, any real or simulated sexually explicit acts, or (ii) expose any sexual organs, or (iii) engage or assist in sexual exploitation or abuse, or sexual services, or (iv) engage in, or observe, sexually explicit communication with another person, including a child, or (v) engage or assist in other sex offenses as defined under the applicable laws, including paying or getting paid for sexual services, controlling a child for sexual exploitation, or grooming a child for sexual purposes, or (c) visually, audibly, or textually, or otherwise, causes, incites, encourages, or instructs any person to facilitate or arrange for, or cause, any child to: (i) engage in, or observe, any real or simulated sexually explicit acts, or (ii) expose any sexual organs, or (iii) engage, or assist, in sexual exploitation or abuse, or sexual services, or (iv) engage in, or observe, sexually explicit communication with another person, including a child, or (v) engage or assist in other sex offenses as defined under the applicable laws, including paying or getting paid for sexual services, controlling a child for sexual exploitation, or grooming a child for sexual purposes; provided that it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification;

		and further provided that any material demonstrably created and/or used strictly for, and only for, legitimate purposes in the relation law enforcement or criminal investigation, medical treatment, or authorized research, education, or media reporting purposes shall not fall within this definition. "**digital non-consensual pornography**" means any material, in any medium, created using any digital or electronic medium, that depicts or describes, of or related to a person, any real or simulated sexually explicit acts, or any sexual organs, or any sexual exploitation or abuse, or any sexual services, where one or more depicted person has not given clear, informed, and voluntary consent for recording, production, possession, marketing, dissemination, purchase, sale, and display of each such material, and it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification; provided that any material demonstrably created and/or used strictly for, and only for, legitimate purposes in the relation law enforcement or criminal investigation, medical treatment, or authorized research and education purposes shall not fall within this definition.
Religious hatred		
Section	**Review and Comments**	**Recommendations**
26	Criminalises speech deemed 'hateful' or 'provocative' towards any religion or its followers. The imprecise language of the provision would risk encouraging human rights abuses by State and non-State actors in the name of religion and would be inconsistent with the requirements of legal certainty under international law. Article 20 of the ICCPR restricts speech on national, racial, or religious hatred that incites discrimination, hostility, or violence. Including merely provocative speech towards a religion or its followers might go beyond what Article 20 intends, verging on blasphemy legislation, for the first time in Bangladesh. Its welcome that this has moved from 'hurting religious sentiment' to identifying 'hateful speech'	This provision should be reconsidered, and any law restricting speech relating to religion should follow international standards, and only restrict such speech if it targets individuals based on their religious and faith background, and if it is considered religious hatred that constitutes incitement to discrimination, hostility, or violence (A/HRC/22/17/Add.4). Further, provide procedural safeguards to protect against its misuse, requiring reasoned judicial approval to proceed for prosecution, and with clear guidelines on the evidentiary standards required for prosecution.

	or 'provocative speech' as the harm. However, these remain very vague, and can infringe on freedom of expression. This risks suppressing legitimate criticisms or debates on religion, religious practices or religious institutions, even where these result in violations of fundamental rights. Jurisprudence interpreting these standards affirms that even speech that offends, shocks, or disturbs may still be protected. Under the DSA, numerous cases were filed including against baul singers, and two 17-year old girls who were held behind bars for up to over a year merely for their online posts which allegedly outraged some people's religious sentiments. Penalising provocative speech will allow such incidents to continue. This provision also does not provide any procedural safeguard, i.e., requiring judicial approval before filing of a case.	
Cyber terrorism		
Section	**Review and Comments**	**Recommendations**
23	Cyber terrorism almost replicating the CSA and DSA on cyber terrorism is extremely broad and vague, and does not refer to the elements in the definition of terrorism formulated by the Special Rapporteur on the promotion and protection of human rights.	Adopt the definition on terrorism set out by Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism as recommended in the OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act in June 2022. The OHCHR recommended that, "counter terrorism offences, including cyber terrorism, 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. An amended section should also be accessible, formulated with precision, applicable to counter-terrorism alone, non-discriminatory and non-retroactive".

Filing Case, Trial and Appeal		
Section	**Review and Comments**	**Recommendations**
41	Seeks to limit spurious cases by permitting only directly aggrieved individuals, their representatives, or law enforcement to file cases. However, some broad aspects of the law might not effectively prevent misuse, as it allows claims of aggrieved status from anyone, for instance in matters related to provocative religious statements. Conversely, this restriction may impede efforts to address cybercrimes, such as hacking, malware, or systemic attacks, which affect larger communities without identifiable victims. Further, independent reports indicate that many cases filed including for vague speech offences under the DSA, when it was in effect, were initiated by law enforcement authorities. Simultaneously, there are concerns that law enforcement occasionally refuse to lodge rape cases, which may potentially translate into sexual harassment reports under the draft ordinance. In instances where victims face intimidation to file cases in the absence of victim and witness protection laws, together with the risk of law enforcement not filing genuine cases, there remains a threat that perpetrators of online harm, including sexual harassment, could evade accountability.	Exclude the wholesale requirement that only aggrieved individuals or law enforcers can file cases, to ensure perpetrators creating cyber security threats such as hacking, malware, or systemic attacks, or of online harms such as sexual harassment do not evade accountability.
Cyber Security		
Section	**Review and Comments**	**Recommendations**
18	The draft penalises illegal access (hacking) or assistance to illegal access to computers, computer systems, digital devices etc. (section 18) but without clarity on its scope, creating risks of over-extending its application to parties without malicious intent. For example, legitimate security testing which is not explicitly exempt may be penalised. The draft does not define hacking. Moreover, the wording is ambiguous regarding whether passive knowledge or indirect involvement, such as unintentional facilitation, should be penalised as assisting illegal access.	Specify what would amount to assistance to illegal access to ensure unintentional facilitation is not penalised, and explicitly exempt those involved in unintentional facilitation and legitimate security testing.
15 and 17	CSO also penalises illegal access to Critical Information Infrastructure (CII) (Section 17) allowing the government to declare what may	Define Critical Information Infrastructure (CII) following the definition adopted by the European Union (EU) or the Organisation for

	constitute CII (section 15) without clear criteria or distinguishing between levels of unauthorised access to CII, i.e., non-sensitive and highly sensitive. It does not include specific mandates for cybersecurity measures, incident response procedures, or technical standards that would strengthen the safeguarding of crucial assets.	Economic Cooperation and Development (OECD). Establish concrete criteria and parameters for classifying Critical Information Infrastructure (CII) and differentiate between CII sectors' sensitivity, ensuring non-sensitive domain access faces lesser legal consequences than highly sensitive areas. To improve technological solutions, include requirements for mandatory cybersecurity measures, incident response plans, and compliance with technical standards following the United States Cybersecurity and Infrastructure Security Agency (CISA), which establishes and enforces security guidelines for critical infrastructure sectors, OECD Recommendations which set out a framework for developing strategies for protecting CII, and EU's NIS Directive that requires essential service operators to implement security measures and report incidents.
19	Obstruction to computers and physical infrastructure in cyberspace is penalised (Section19) but the broad definition of the term "obstruct" may penalise minor infractions and legitimate security or privacy actions.	Precisely define the term "obstructs" to differentiate between illegal obstructions and legitimate security or privacy activities.
21 and 22	Cyber fraud is penalised (Section 21) with "fraud" being vaguely defined as access "without rights or in excess of rights or unauthorised practice", with no clarity on the grantor of rights or breach criteria. Cyber forgery is addressed (Section 22) using phrases such as "deliberate or intentional", complicating proof of intent, and leaving room for subjective interpretation, and differing legal conclusions.	Delineate who holds the authority to grant access rights, and specify what constitutes an "unauthorised practice" to clear ambiguities around fraud and forgery. Define "deliberate or intentional" actions and provide parameters clearly to reduce subjectivity and ensure consistency in penalising cyber forgery.
Enforcement Actions		
Section	**Review and Comments**	**Recommendations**
2 (1) (z)	The draft intending to regulate the "cyberspace" defines it broadly, aiming to cover a wide range of digital and technological elements. By attempting to include almost every modern technology, it dilutes the focus on what specifically constitutes "cyberspace", "digital devices", or "virtual" realms. Including diverse technologies, such as quantum	Related technologies and systems should be precisely defined and categorised into separate groups, for greater insight and utility.

	computing, blockchain, and social media among others, alongside one another may lead to confusion, as each belongs to distinct domains with unique characteristics and applications.	
	Technical Expertise and Resources: The draft fails to outline the technical proficiency and resource allotment required for law enforcement to effectively identify, prevent, and manage infractions concerning cybercrimes.	Ensure the law specifies the qualification and the technical proficiency required for the law enforcement officers to effectively identify, prevent, and manage infractions concerning cyber crimes.
	Sentencing: The draft, similar to its predecessors, the Cyber Security Act, Digital Security Act, and section 57 of the ICT Act, and all criminal legislations in Bangladesh, provides for punitive actions for offences under it, and lacks sentencing guidelines, raising concerns over disproportionate and inconsistent sentencing for convictions under the law.	Include non-punitive actions for less severe crimes. Establish clear sentencing guidelines to ensure consistent, fair, and proportionate penalties. This should comprise categorising the offences based on severity, aggravating and mitigating factors, sentencing range, non-custodial penalties such as community services, probation, or fines.
2. Procedures		
Section	**Review and Comments**	**Recommendations**
8	The grounds for blocking content remain the same as earlier (under the CSA and the DSA) and include "undermining integrity, economic activities, security, defence, religious values, or public order". These terms are open to subjective interpretation and possible arbitrary application, with significant scope for free speech restrictions and surveillance. Significant powers are given to the Director-General of the Cyber Shurokkha Agency, and Law Enforcement Agencies to recommend blocking to BTRC or the ICT Division, without any independent oversight. This risks the DG and LEAs exercising unchecked authority, resulting in potential abuses. Allowing both the BTRC and the ICT Division to handle blocking creates major enforcement concerns due to unclear responsibilities and jurisdictions. The requirement to request a Government body (ICT Division) to block content and to inform the government about any blocked content also keeps the scope for surveillance open, similar to what we have seen under the CSA and the DSA.	Remove the wholesale and unfettered blocking powers given to the DG under vague grounds. Ensure a body with organisational independence from the Government deal with blocking content. a. Define blockable content categories based on permissible restrictions on freedom of expression under the International Covenant on Civil and Political Rights. b. Ensure blocking authorisation through court orders, adhering to procedural safeguards, which must include: ● Allowing Internet Service Providers to contest blocking applications. ● Providing users with post-factum rights to challenge blocking decisions, with visible notifications explaining the reasons and involved parties in blocked content, along with clear information for appeals or redress. ● Ensuring prompt reviews by impartial courts. ● Limiting the duration of blocking to avoid prior censorship.

34	**Search, and seizure with warrant:** The draft allows police officers to intercept communications or obtain traffic data with search warrants if they have “reasons to believe” an offence under this law is committed or might be committed. However, it does not require them to specify the exact actions they intend to take under the warrant. Furthermore, the lack of clear guidelines on what constitutes "reason to believe", leaves room for subjective interpretation.	Require police officers to specify the exact actions they intend to take and methods they intend to use when seeking a warrant, ensuring transparency and accountability. Set precise criteria for what constitutes "reason to believe" an offence is or may be committed to reduce subjective interpretation. Implement an independent oversight mechanism to review and approve warrants based on these criteria to safeguard against potential misuse, and ensuring privacy protections.
35	**Search and seizure without warrant:** The draft allows police to enter and search any location without a warrant based on mere suspicion that a cyber attack on Critical Information Infrastructure (CII), hacking etc has occurred, is occurring, might occur, or if evidence might be compromised. The draft does not define either "hacking" or "cyber attack" and the government retains the discretion to declare what constitutes CII without providing clear criteria or distinctions between varying levels of unauthorised access to CII, whether it involves non-sensitive or highly sensitive information, keeping a broad scope for misuse. Since allowing to search and seize extend to any person’s home, this draft conflicts with constitutional rights to privacy of home, which can be restricted only for security of the state, public order, morality, or health— and given the grounds under this provision are undefined, not all acts labelled as cyber attacks or hacking may meet constitutional standards, potentially leading to unjustified actions.	To align with constitutional standards, it is crucial to define the grounds allowing searches without warrant, limiting the criteria to the permissible limitations on privacy of home and correspondence.
35	**Arrest without warrant:** Permitting arrest based on mere suspicion creates scope for misuse. The draft, following the CSA and previously the DSA, lacks specific procedures and guidelines to ensure actions are grounded in legitimacy, not arbitrary decisions. This power was abused regularly for arrests of dissenters including children under the CSA, DSA, and ICTA.	Restrict arrest without warrant to only offences that pose a direct threat to body and personal safety. Provide specific procedures and guidelines that must be adhered to, ensuring that any actions taken for addressing suspicions of such threats are based on legitimate grounds rather than arbitrary decisions.

32	**Investigations:** The Draft does not provide any specific grounds for when Tribunals can allow continuation of investigations beyond the finite time periods.	Provide specific and precisely defined grounds when Tribunals can allow continuation of investigations beyond the finite time periods, ensuring any exceptions are not routinely exercised.
12	**Authorities:** The National Cyber Shurokkha Council, a government body, holds significant authority including to block content, and control and supervise the digital forensic labs among others. The National Cyber Shurokkha Council, chaired by the Prime Minister or the Chief Advisor, includes 17 members from various government and autonomous entities. However, these members lack cybersecurity or technology backgrounds, raising questions about their ability to fulfil their roles in guiding the Agency in implementing the Ordinance. The Council's inclusion of security agencies such as the NTMC and NSI permits surveillance activities similar to the CSA and its predecessor, DSA. There is no requirement for independent oversight or court approval of actions by either of these bodies, threatening free speech and granting them broad surveillance powers.	a. Establish the independence of the National Cyber Shurokkha Agency from the government, ensuring organisational autonomy, defining its functions more specifically, and creating a mechanism to hold them to account. Similarly, establish the independence of the Cyber Shurokkha Council ensuring clarity on its role in guiding the Agency. Include members with cybersecurity or tech expertise in the NCSC, and ensure independent oversight of the NCSA. b. Establish independent digital forensic labs separate from the government for ensuring independence and checks and balances
Trial Procedures:		
	Concerns	**Recommendations**
	a. The draft remains silent, similar to the CSA and the DSA, regarding the procedures to be followed if a child is accused of committing an offence under this law. This raises concerns among practitioners, as typically, the provisions of the Children Act would apply in such cases. However, the draft explicitly states that it would take precedence over other laws. In cases under the DSA thus far, Tribunals have not provided clarity on which law should be applicable. b. Children who are accused under the CSA are tried before the Nari O Shishu Nirjaton Domon Tribunal, and this practice is expected to be followed for child accused under the draft Ordinance. The presiding judges in these Tribunals are not equipped with specialised training in cyber or technology-related issues.	a. Ensure that the provisions of the Children Act take precedence over the draft Ordinance. b. Ensure that cases involving children accused of offences under the CSO or other laws relating to internet crimes are tried before Cyber Tribunals, presided over by judges who have received specialised training in cyber and technology-related matters, as well as in children's rights. c. Ensure admission of digital forensic evidence is made mandatory. d. Make examination of digital forensic experts in court mandatory to ensure transparency and credibility of their reports.

	This lack of specialisation poses a significant challenge in ensuring that cases involving children are handled with the appropriate sensitivity and expertise required. **c.** The draft following its predecessors do not require mandatory admission of digital forensic evidence for prosecution of an accused, creating inconsistent standards for evidence admissibility and undermining fair trials.	
Cybersecurity and cyber safety		
	Concerns	**Recommendations**
	Integrating cybersecurity and cyber safety measures into a single legislation may lead to disproportionate emphasis on punitive actions related to cyber safety, rather than preventive cybersecurity measures. Additionally, merging these laws can result in ambiguous or conflicting legal provisions, as cybersecurity and cyber safety require distinct approaches. This complexity may pose challenges in interpreting and applying the laws effectively	The governance of cybersecurity and cyber safety should be addressed through separate legislative frameworks to minimise complexities in interpretation and enforcement. The draft Ordinance addresses only a portion of the broader aspects encompassed by cyber safety laws. Consequently, dedicated consultations with experts should be convened to formulate a separate and comprehensive law in this area.