The Daily Star
FOUNDER EDITOR: **LATE S. M. ALI**

Secretariat fire needs answers and action

How can such a vital government complex be so unsafe?

We are alarmed by the massive fire that ravaged parts of a nine-storey building within the Secretariat complex in Dhaka. According to a report by this daily, the fire—which broke out in the early hours on Thursday—persisted for nearly 10 hours, fully or partially damaging the offices of at least five ministries and divisions across multiple floors. Among the casualties were not just furniture and office equipment, but many documents and records as well. Tragically, a firefighter also died while setting up hose pipes as he was run over by a truck before traffic to the area was closed. The incident has naturally shocked many, as it laid bare a lack of security in one of the country's most important public infrastructures.

The question is, was this merely a result of electrical malfunctions, or was there something more sinister? Since the incident, a number of theories have surfaced as officials and the public try to wrap their head around what happened. One theory that is making the rounds at present is a suspicion of foul play, fuelled particularly by Adviser Asif Mahmud's revelation that evidence of significant financial irregularities was among the lost documents. The student platform that spearheaded the July uprising also called the incident "an act of sabotage," while Bangladesh Administrative Service Association hinted at deliberate arson—allegedly orchestrated by corrupt bureaucrats linked with the Awami League to derail the ongoing reform efforts and to destabilise the government. However, calmer heads within the administration want to wait before pointing fingers as investigations are underway.

Regardless of the suspicions floating around, one thing that we can say with certainty is that there were lapses in fire security that contributed to the catastrophe. Reports reveal that firefighting efforts at the Secretariat complex were hindered by significant logistical challenges both outside and within the building, delaying the firefighters' response time and efforts. We also need to talk about why, in this day and age, a digital record-keeping system that could minimise the loss of important records remains underutilised. This may be a testament to the corruption and inefficiencies that plagued the previous regime's digitisation drive, but a transition to digital archiving should have been a priority for the interim government. Going forward, we must address these safety issues to safeguard critical infrastructure and information.

As we await the findings of investigations, which we expect the probe committees to deliver as soon as possible, it is vital that the authorities take lessons from this latest setback for the administration that is already struggling amid protracted unrest over civil service reforms and decisions surrounding promotions and placements. The Secretariat also must adopt robust fire safety measures. Security protocols should also be thoroughly reviewed and properly upgraded. Whether the fire is a result of conspiracy or complacency, it has exposed vulnerabilities that threaten not just the administration but the public trust in our institutions. We must prevent a repeat of such incidents in the future.

We must improve dengue management

Bangladesh can learn from Kolkata's success story

The dengue situation in Bangladesh remains alarming, with multiple cases still being reported in late December. As of Thursday, 100,558 people were hospitalised due to dengue this year, including 9,089 in December alone. While the record-breaking 1,705 deaths of 2023 were not repeated, the 565 deaths recorded this year represent the second-highest toll in recent years. Also, the decline usually seen in winter cases has not occurred this year, with at least one death reported on all but two days this month, underscoring the gravity of the situation. Unfortunately, the government's response continues to be inadequate in addressing this crisis.

Despite repeated calls for action, its dengue management efforts have fallen short. Regular mosquito control drives in Dhaka and other cities were poorly conducted, and no effective hotspot management measures were implemented. Meanwhile, hospitals outside Dhaka, ill-equipped to handle critical dengue cases, were overwhelmed. Experts have also raised concerns about the ineffectiveness of the pesticides used.

Understandably, the government's mosquito control drives were disrupted by the political transition in August. After the removal of elected ward councillors on September 26, regional executive officers took over their duties, but the momentum needed to combat dengue was lost. Ward councillor offices, which traditionally manage mosquito control among other services, became largely inactive during this crucial period. So to tackle dengue more effectively next year, the government must focus on strengthening city corporations and ward councillor offices. In this regard, Bangladesh can draw valuable lessons from Kolkata's successful dengue management model.

Reportedly, the Kolkata Municipal Corporation (KMC) runs a robust, year-round vector control programme across its 144 wards and 16 boroughs. Their approach integrates expert management, including entomologists, with ground-level implementation by Rapid Action Teams (RATs) and field workers. These teams proactively monitor and eliminate mosquito breeding sites while conducting awareness campaigns. KMC uses a ward-based database to identify high-risk areas, and when a dengue case is reported, RATs respond swiftly by inspecting and clearing breeding sites in the patient's home and 50 surrounding houses within 24 hours, extending the search to another 50 houses later. Data from diagnostic centres is also promptly utilised for targeted action.

Bangladesh must adopt similar measures to curb dengue. Declaring dengue a reportable disease from January 2025, combined with proactive surveillance, hotspot management and community awareness, can significantly reduce the spread of the disease and save lives.

THIS DAY IN HISTORY

First commercial film screened

On this day in 1895, the world's first commercial film screening took place at the Grand Cafe in Paris, France. The film was made by Louis and Auguste Lumière.

DSA's shadow over the Cyber Protection Ordinance

Kallol Mustafa
is an engineer and writer who focuses on power, energy, environment and development economics. He can be reached at kallol_mustafa@yahoo.com.

KALLOL MUSTAFA

In the face of widespread criticism, the Sheikh Hasina government enacted the Cyber Security Act (CSA), 2023 by repealing the Digital Security Act (DSA), 2018, which had been used to suppress freedom of expression in Bangladesh. But the old repressive clauses were retained in the CSA. The interim government, which came to power on the back of a student-led mass uprising in August, is revoking the controversial CSA and enacting the Cyber Protection Ordinance (CPO), 2024. The draft, already approved by the Advisory Council, was made available online for review for only three working days. Issuing such an important ordinance without sufficient analysis and inclusive feedback from relevant stakeholders carries the risk of repeating history.

The Cyber Protection Ordinance elaborates the definition of cyberspace, incorporating emerging technologies including artificial intelligence. The definition of cyber protection includes the citizens' right to 24/7 internet access and data privacy. The ordinance mentions that eight controversial sections of the CSA have been cancelled along with the ongoing cases under it. In some cases, the terms of sentence have been reduced from the previous equivalent sections, the number of non-bailable clauses has been reduced, and anyone other than the person directly aggrieved or his/her appointee or a law enforcement member is barred from suing under the ordinance.

These are all positive changes. However, some provisions of the DSA (and the CSA) have been included in the CPO, through which civil rights and freedom of expression might be undermined. For example:

1. Similar to Section 8 of DSA and CSA, Section 8 of CPO empowers the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block content that may undermine "national unity," "economic activity," "security," "defence," "religious values" or "public order," on request of law enforcement agencies and the director-general of the National Cyber Security Agency. There is no provision for disclosure of blocking statistics, judicial review, and explanation of why a content would be removed or blocked. If law enforcement agencies or bureaucrats are given the power to determine whether an online news report or content is harmful for "national unity," "economic activity," "security," "defence," "religious values" or "public order," there is always a risk of abuse. I think only in specific cases of "communal violence" can any content block be authorised, though there should be a mechanism for judicial review. That is, to prevent communal violence, there should be a system such that the judiciary will regularly review what content the BTRC has removed or blocked, and if any abuse is proven, the responsible person will be punished.

VISUAL: **SALMAN SAKIB SHAHRYAR**

2. Section 25 (1) of DSA (and of CSA) made it an offence to "transmit, publish or disseminate any information with intent to annoy, insult, defame or degrade any person." Section 25 (1) of CPO also makes it an offence to transmit, publish or disseminate any information with intent to insult, harass or defame a person. This section specifically recognises "cyberbullying" as a crime. It is being argued that this provision has been included specifically for the protection of women and children. But the ordinance does not specifically mention women and children. What's the guarantee that people will not be oppressed by this provision, much like the defamation clause of the DSA?

Cyberbullying is a term that can be used to label any form of criticism that may be deemed to harass or abuse people. Acts considered to be cyberbullying, as defined in CPO, include posting false or harmful information, insulting messages, rumours or defamatory content. Just as through the DSA people were oppressed and harassed on the charges of "defamation" or "spreading false information," Section 25 (1) of CPO will also create a loophole to oppress and harass people on the charges of "cyberbullying." Moreover, every online platform has various mechanisms to tackle bullying, like blocking, reporting, etc. UNICEF has urged to enhance digital literacy, use various tools of online platforms and, where necessary, use the existing relevant criminal laws of the country to prevent cyberbullying. This is why rehabilitating the defamation clause of DSA in the name of protecting women and children from cyberbullying is not acceptable.

3. Section 28 of DSA (and of CSA) criminalised hurting religious "values" or "sentiments," which was used to harass and oppress people during the previous regime. This DSA section has been incorporated in the CPO, in a slightly modified form, as Section 26. The change includes the issue of spreading false information and hatred by hacking into another person's device. But distinguishing between genuine debate around religion or hurting religious sentiment is a delicate matter. If this is to be resolved through police, law and court, there is a chance of oppression and abuse. Therefore, this issue should be resolved socially through discussion and debate. Dragging the state into matters of religious faith is not beneficial at the end of the day. Therefore, Section 26 should be scrapped. If someone illegally accesses another person's device and spreads misinformation regarding religion, they can be punished under Section 18 of CPO for hacking.

4. Section 43 of DSA (Section 42 of CSA) empowered police to search, seize and arrest without warrant. This section has been included as Section 35 of CPO, with the provision of a new sub-section that provides that a person arrested without warrant will be produced before the nearest magistrate or tribunal "without delay." But this does not solve the core problem of this provision, which is the power given to the police to "search, seize and arrest without a warrant."

5. As in Section 54 of the repealed DSA (Section 53 of CSA), Section 47 (3) of CPO makes "legitimate" cyber equipment accompanying "forfeitable" cyber equipment used in unlawful activities also forfeitable. This provision is completely unreasonable and can be used to harass individuals and institutions. If a piece of cyber equipment is legitimate and not used in the commission of a crime, there is no reason to seize it just for accompanying a piece of "forfeitable" cyber equipment.

6. The definition of "cyber protection" includes the citizens' right to 24/7 internet access and data privacy, but there is no mention of the punishment for violating these rights in the ordinance. As a result, these rights are likely to remain mere promises.

The people of Bangladesh have been deceived time and again in the name of amendment to oppressive laws. Section 57 of the Information and Communication Technology (ICT) Act, 2006 was repealed, but the provisions of that repealed section were included in the DSA. Then the nine sections of DSA that were identified as a threat to independent journalism and freedom of expression were incorporated in the CSA. This practice must not be allowed to continue through the Cyber Protection Ordinance, 2024.

Proper audits can ensure social compliance in the RMG industry

Dr Saika Nizam
is project coordinator of Occupational and Environmental Health at Bangladesh University of Health Sciences.

Prof Peter Hasle
is project leader of Global Sustainable Production at the University of Southern Denmark.

Sarmin Sultana
is PhD student in Occupational and Environmental Health at Bangladesh University of Health Sciences.

Julie Bundgaard
is PhD student in Global Sustainable Production at the University of Southern Denmark.

SAIKA NIZAM, SARMIN SULTANA, JULIE BUNDGAARD *and* **PETER HASLE**

The ready-made garment (RMG) industry of Bangladesh plays a significant role in the country's economy as well as in the global apparel market. The well-being of Bangladeshi RMG workers has long been a topic of concern for stakeholders in the international supply chain. Since 2011, the UN Guiding Principles on Business and Human Rights has served as an ethical compass for global fashion brands and other businesses to protect human rights in the context of business operations. Simultaneously, the formulation of buyers' code of conduct (CoC), particularly in countries like Bangladesh, has had a crucial role in defining guidelines and expectations for suppliers to ensure that they adhere to social compliance standards.

The horrific collapse of Rana Plaza in 2013 further pushed for stricter regulations and much more extensive audit practices to prevent similar tragedies in future. Subsequently, social compliance audits expanded greatly with international brands doing audits of their CoC, and multistakeholder initiatives such as the Business Social Compliance Initiative (BSCI) and Supplier Ethical Data Exchange (Sedex) doing third-party audits.

Social compliance audits are the primary tools to monitor working conditions and prevent human rights abuses in RMG factories worldwide. Most RMG factories experience many audits over the year. These audits seek to secure safety, health, wages, working hours and freedom of association of the workers.

However, audits are expensive for both buyers and suppliers, and overlapping audits from different bodies can cause audit fatigue among RMG factories.

In our research, we have looked at audits in 10 RMG factories as case studies, and the results indicate that despite problems with the current social compliance practices, some factories found ways to achieve benefits from audits.

Factories mainly expressed satisfaction with the audit system, but many compliance managers experienced audit fatigue due to multiple and parallel audits; some also concealed non-conformities from auditors. Generally, audit reports identify non-conformities related to the most visible safety and health issues, such as personal protective equipment, needle guards, and electrical safety, together with issues related to payment and working hours. Ergonomics risk factors such as working postures and heavy lifting as well as freedom of association are rarely included in audits or audit reports.

Workers' voices influence audits to a limited degree. Auditors don't give the workers a real chance to point to critical issues, and if they do, the issues are not necessarily brought to the attention of the management.

The factories we included in our research revealed two different approaches of responding to audit practices:

1) A low road, where the factory considers buyers' and audit requirements as unfair and costly. They believe that cost reduction is the only way to be competitive. Therefore, they go for an absolute minimum standard of compliance, often with elements of window dressing. In this group of factories, we noticed the tendency to make informal arrangements with the auditors. Visits to these factories showed limited investments related to working conditions, but also to technology and operations. Overall, these factories have low management capacity both in general and related to social compliance.

2) A high road, where factories take a systematic and proactive approach, establishing management systems with clear procedures for both operations and social compliance. These factories believe that they can stay competitive through high quality and high productivity developed with a motivated workforce as well as continuous improvement of technology and work organisation. They use audits as a source for identifying additional possibilities for improvement. These factories turned out to be affiliated to the Better Work programme, a flagship initiative of the International Labour Organization (ILO) and International Finance Corporation (IFC).

Our research highlighted that factory management is usually the driving force behind choosing the low or the high road of social compliance practices. Irrespective of the compliance strategy followed, we found that managements as well as the auditors have neglected certain occupational safety and health (OSH) issues encompassing ergonomic demands for workstation design, training in preventive measures, reduction of highly repetitive work and psychosocial climate such as prevention of various forms of harassment.

We propose the following steps to address these gaps:

1) Dissemination of research results and exchange of experience among peer factories.

2) Stronger involvement of buyers and brands in the welfare of workers. One reason for the selection of the low road practice is expression of limited genuine interest in social compliance among the buyers.

3) Inclusion of neglected problems in audits such as ergonomics, workers' voices and stronger quality control of audits to avoid conflicting interests.

Audits should not only rectify current problems but also support the development of a strong preventive safety culture. Our study showed that it is possible for a factory to reach a high level of social compliance and at the same time be fully competitive by using audits to improve conditions for both workers and the business.

This article summarises key findings from a research titled "Social Compliance Audits in the Garment Industry in Bangladesh: Present Practice and Future Perspectives (2024)." The research was conducted jointly by Bangladesh University of Health Sciences and the University of Southern Denmark.

The Daily Star Reg. No. DA 781 | **EDITOR & PUBLISHER: Mahfuz Anam** Printed by him on behalf of Mediaworld Ltd at Transcraft Ltd, 229, Tejgaon Industrial Area, editor@thedailystar.net | **Registered & Head Offices:** The Daily Star Centre 64-65 Kazi Nazrul Islam Avenue, Dhaka-1215 Phone: 09610222222 | **Newsroom:** Fax- 58156306 reporting@thedailystar.net | **Advertisement:** 01711623910 advertisement@thedailystar.net GPO Box: 3257 | **Subscription:** 01711623906 | thedailystar.net bangla.thedailystar.net/