

## Delhi, Dhaka must dial down the heat

### Diplomatic tensions lurching towards a crisis

We share our foreign ministry's concern over the recent breach of the diplomatic zone housing the Bangladesh High Commission in New Delhi. To our surprise, India's external affairs ministry characterised the incident as a trifling affair involving 20 to 25 people protesting the killing of a worker in Mymensingh. To the diplomats inside the Bangladesh mission, who witnessed the slogans and the thinness of the security cordon, the incident appeared not as a minor nuisance but as a considerable lapse in protection.

Foreign Adviser Touhid Hossain has rightly asked how a band of activists from a Hindu extremist organisation managed to penetrate deep into one of New Delhi's most fortified areas without permission, particularly when the building is not located on the outskirts? The protesters issued death threats to the high commissioner who resides there with his family. This incident has added a fresh layer of tension to the already fraught relationship between the two nations.

It bears repeating that for many years, the bond between India and Bangladesh was cemented by New Delhi's unwavering backing of Awami League. With the party now overthrown and its leader issuing incendiary comments from exile in India, that foundation has taken a serious hit, giving way to a void filled with mutual suspicion. Dhaka views New Delhi as a sanctuary for fugitives conspiring against Bangladesh. The interim government recently pointed to the killing of Sharif Osman Hadi, a leader of the 2024 uprising, by a suspect who reportedly slipped across the border. New Delhi, meanwhile, sees a neighbour sliding into majoritarian chaos. It views the interim government's handling of minority safety with scepticism, dismissing Dhaka's assurances as inadequate.

Last week, this diplomatic estrangement played out through reciprocal summonses. On December 14, the foreign ministry in Dhaka called in the Indian high commissioner to issue a rebuke regarding "anti-Bangladesh activities" allegedly orchestrated by fugitive Awami League figures on Indian soil. Having summarily rejected Dhaka's assertion, India's external affairs ministry waited just three days before summoning the Bangladeshi high commissioner in New Delhi. There, Indian officials registered their own concerns over a "deteriorating security environment" across the border.

Although a report presented by India's parliamentary standing committee on external affairs on December 18 identified the political shift in Bangladesh as New Delhi's "greatest strategic challenge" since 1971—calling for an immediate "recalibration" of ties—the Indian government appears to be heading in the opposite direction.

The economic fallout of this crisis is already tangible. India has drastically restricted shipments through land ports and curbed general visa issuance since August 2024; for its part, Bangladesh has imposed curbs on Indian yarn imports. Such decoupling is painful for businesses and individuals on both sides. Geography dictates that the two countries cooperate on everything from commerce to security. Yet the rhetoric is hardening, and the danger is that it is crowding out pragmatic diplomacy. Bangladesh's demand for an explanation regarding the security breach in Delhi is legitimate, so too are India's concerns about the safety of its missions in Bangladesh.

To prevent this downward spiral, New Delhi must look beyond the prism of its deposed allies. Normalisation requires acknowledging that the political landscape in Dhaka has fundamentally shifted. India needs to do far more than issue statements on minority safety—it must engage constructively with the new power centres.

## An alarming breach of citizens' data

### Fake e-Apostille websites expose our digital governance's flaws

We are alarmed by the leak of sensitive personal data of at least 1,100 citizens through a fake e-Apostille website, which is a stark reminder of how vulnerable citizens' data remains in the country. Reportedly, national identity cards, passports, marriage certificates, educational records, trade licences, and business contracts—documents that define an individual's legal and personal identity and are required for studying abroad, employment, or business purposes—were left openly accessible on a fraudulent platform posing as a government service.

This fake website closely resembled the government's official e-Apostille portal, which digitally authenticates government issued documents. The official portal is operated under the myGov platform of the ICT Division's Aspire to Innovate (a2i) programme. The fake website used a similar structure and name but ran on a different domain. It not only issued fake e-Apostille certificates but also allowed anyone to access other people's documents without much effort. In other words, without any form of identity verification or additional authorisation, a user could access another person's sensitive documents. This is worrying. Reportedly, many victims of the data breach applied through shops or intermediaries, a common practice given the complexity of the procedure. But whether they applied themselves or via intermediaries is irrelevant. The fact that such a large volume of sensitive data could be uploaded, stored, and accessed on a fraudulent platform points to systemic weaknesses in oversight, public awareness, and digital governance.

Unfortunately, this data leak is not a one-off incident. Previous allegations of data leaks involving platforms such as Surokkha—the government's Covid-19 vaccination management system—and reports of citizens' data being sold on the dark web suggest a persistent pattern of breaches. Leaks of passports, NIDs, and marriage certificates open the door to identity theft, fraud, harassment, and serious personal security risks. Women, in particular, are more vulnerable to the misuse of such information. Alarmingly, at least six fake domains posing as myGov and e-Apostille services have been discovered. These look-alike websites, designed to extract personal data and potentially commit financial fraud, not only endanger citizens but also erode trust in legitimate government platforms.

The government must prioritise and protect citizens' personal information through stronger security standards, independent audits, swift takedown of fake platforms, legal action against those involved, and public awareness campaigns. Without such measures, Bangladesh's push towards digital governance will not succeed.

## Unchecked violence casts a shadow on our economy



### MACRO MIRROR

Dr Fahmida Khatun is executive director at the Centre for Policy Dialogue. Views expressed in this article are the author's own.

### FAHMIDA KATUN

The recent wave of violence has revealed a deeply worrying trend in public life. Following the announcement of the 2026 national election by the Election Commission of Bangladesh, a young political leader, Sharif Osman Hadi, was shot in broad daylight on December 12 by miscreants. Six days later, he succumbed to the bullet injuries while undergoing treatment in Singapore. The killing of Hadi sends a clear message that speaking differently has become dangerous. This is not confined to politics. Mob attacks on two prominent newspapers and two cultural institutions, and the lynching of a minority citizen in public, are examples of how the country's atmosphere has been marked by violence and fear.

The attacks on *The Daily Star* and *Prothom Alo* are not just against their infrastructure. They are attacks on the idea that citizens have the right to know, question, and disagree. The free press holds up a mirror to society. When that mirror is smashed, those in power go unchallenged, and falsehoods spread easily. The assault on cultural institutions such as Chhayanaut and Udichi is equally alarming. These spaces keep alive values of tolerance, human dignity, and progressive thinking. Songs, poetry, and art shape our conscience. That is why they are often targeted first. The killing of a garment factory worker, Dipu Chandra Das—after he was beaten and his body was set on fire in Bhaluka, Mymensingh, allegedly by his co-workers and a mob falsely accusing him of hurting religious sentiments—is another example of intolerance when people took the law into their hands.

Together, these incidents portray to the world that intolerance is growing and public protection is weakening. A society that silences its voices, crushes its culture, and fears difference may still function, but it slowly loses its humanity, confidence, and hope for a better future.

These attacks took place while a functioning government was in place in Bangladesh. This realisation has shaken the conscience of peace-loving and

progressive people, as many see these incidents as signs of a deeper crisis of values and erosion of confidence that now affects politics, governance, and the economy of the country.

Particularly, the loss of Sharif Osman Hadi resonates deeply in a society where youth symbolise both hope and possibility. That this tragedy occurred just as the country began preparing



FILE VISUAL: SALMAN SAKIB SHAHRYAR

for a national election has intensified emotions further. In many countries, electoral processes bring anxiety and confrontation. Pre-election violence is not uncommon in Bangladesh, yet the current situation is distinct. Since the interim government assumed office in August 2024, law and order have appeared increasingly vulnerable to mob violence. An environment has been created where intimidation, vandalism, and public disorder have become disturbingly normalised.

The key question is why such violence continues under a government whose primary mandate is to stabilise the country and ensure a credible electoral process. This erosion of authority is deeply troubling, for it suggests the weakening of the government's moral and institutional grip.

The central issue, therefore, is the response to violence. In this regard, the government's performance has been hesitant and insufficient. Statements have been issued, assurances have been made, yet tangible outcomes remain

house rent, education fees, and healthcare expenses consume an ever-larger share of household income. For wage earners and small traders whose incomes have not kept pace with prices, life feels increasingly fragile.

While the interim government deserves due credit for rescuing the economy from its fragile condition left by the former government in 2024, through several decisive measures, there are still deep wounds in the economy. For example, reform measures are ongoing to discipline the banking sector and strengthen the foreign reserves. The external sector has improved, with higher exports, imports, and remittances compared to fiscal year 2024. The foreign exchange reserve has been improving from a situation of constant decline and now stands at \$27.88 billion as of December 18, 2025, compared to \$19.95 billion on December 18, 2024. However, the economy is yet to recover from low growth, high inflation, and subdued investment.

Although average inflation has eased from 11.38 percent in November 2024 to 8.29 percent in November 2025, prices of essential goods remain high relative to income. For many, daily life has not become easier despite official signs of improvement, as wages have not increased. Wage growth remained stagnant at 8.04 percent in November 2025, down from 8.1 percent in November 2024, exerting downward pressure on household purchasing power.

Employment conditions are worrying. Formal job creation has slowed, while informal and short-term work has expanded. Many firms are avoiding permanent hiring, and underemployment is widespread. More than 20 percent of youth aged 15-29 are not in education, employment, or training (NEET), revealing deep labour-market stress. Young people entering the labour market face increasing difficulty finding stable and decent jobs, which contributes to frustration and social tension.

Private investment is weak. Private-sector credit growth fell to a record low of 6.23 percent in October 2025, reflecting persistent investment weakness. Domestic investors are delaying expansion plans, focusing on survival rather than growth amid a high cost of doing business and uncertainty. Foreign direct investment remains modest at less than one percent of gross domestic product, with new and existing investors cautious about investing. This is a major concern, as Bangladesh needs investment to diversify its economy and create higher quality employment.

Although Bangladesh is widely recognised for its economic resilience and development achievements, images of mob violence and uncertainty over governance raise concerns among international partners and investors. In an interconnected world, political stability is inseparable from economic credibility. How Bangladesh navigates this moment will shape perceptions in the months ahead.

The way forward must therefore be grounded in both political responsibility and economic prudence. What is at stake now is public confidence and safety. Citizens want to feel that the state stands firmly on their side, that their safety matters, that laws apply equally, and that no one is beyond accountability. As the nation awaits a democratic transition through an election on February 12, 2026, the immediate priority of the interim government must be to restore law and order to protect citizens.

## How to ensure publicly funded software serves the public



Sahadat Hossain is a business consultant and ICT strategist. He can be reached at hisahadan@gmail.com.

### SAHADAT HOSSAIN

Bangladesh has taken a bold step in declaring that software developed with public funds will be treated as a national asset. The ICT Division's draft National Source Code Policy 2025, with its tagline "Public Money, Public Code," seeks to embed ownership, transparency, security, and reusability into the country's digital governance. It is a visionary initiative, but one that requires careful scrutiny.

The policy applies to all software systems, applications, Application Programming Interfaces (APIs), and digital services developed or acquired through the national budget, foreign loans, or donor financing under government projects. It is mandatory for ministries, departments, statutory bodies, and autonomous and semi-autonomous organisations. At its core, the policy requires that all source code be deposited in a central repository managed by the Bangladesh Computer Council. No software can be deployed in production until its code is stored there, ensuring traceability, auditability, and security. It also introduces the principle of "Reuse First," obliging agencies to reuse existing solutions before developing new ones and to justify in writing if reuse is not possible. Most significantly, the policy declares that government-

owned source code will be open by default, unless exempted for national security, defence, or privacy reasons. Even exempted systems must be registered and reviewed periodically.

The merits of this approach are clear. Transparency will allow citizens to see how public money is spent and what code is produced. Reusability will save costs and prevent duplication. Security will be strengthened through centralised oversight, vulnerability scanning, and licence compliance.

Innovation will be encouraged as open code fosters collaboration between government, academia, and industry. In many ways, the policy aligns Bangladesh with broader international movements towards open-source and public-code principles. India's open source policy encourages government adoption of open source software, and European Union institutions have open source software strategies and collaborative platforms that promote sharing and reuse of publicly developed code and software.

Nevertheless, risks remain. Many agencies lack skilled developers to follow secure coding guidelines and Continuous Integration/Continuous Delivery (CI/CD) pipelines, raising the danger of superficial compliance. Over-

centralisation could create bottlenecks and reduce agility. Exemptions for national security may be overused, thereby undermining transparency and openness. Contractors may resist open licensing, fearing the loss of commercial advantage. And without proper documentation, open code risks becoming "abandonware"—technically open but practically unusable.

Bangladesh has already seen how fragile digital governance can be when national databases are mismanaged. In 2023, a major breach exposed the data of over five crore citizens, shaking public trust in digital systems. That episode serves as a cautionary reminder: openness alone is not enough. Without strong documentation, oversight, and security protocols, even well-intentioned initiatives can falter and compromise national assets.

Bangladesh can learn from global experiences. The European Union emphasises documentation and community support, recognising that open code without documentation is meaningless. South Korea integrates open-source adoption with strict security audits, showing that openness must be paired with cybersecurity rigour. Singapore's GovTech runs a government technology stack where reusable components are shared across ministries, proving the importance of modular design and developer training. In the Global South, countries like Brazil and Kenya have adopted public code principles but struggled with sustainability, as projects often collapse after donor funding ends. Bangladesh must ensure long-term maintenance budgets and

community engagement.

To make the policy effective, Bangladesh must invest in capacity building, training developers and auditors in secure coding and open-source practices. Documentation standards must be mandated, ensuring that code is not just open but usable.

While a central repository is useful, agencies should retain autonomy to manage linked sub-repositories to avoid bottlenecks. Exemptions must be clearly defined and independently overseen.

Contractors should be incentivised to contribute to open code through recognition and reuse credits. Sustainability must be ensured through dedicated budgets for maintenance and updates. Finally, Bangladesh should build global partnerships with Japan, Korea, and Singapore to adopt best practices and strengthen regional networks for open government software.

The draft National Source Code Policy 2025 is visionary in recognising that software built with public money is a public asset. It seeks to embed transparency, security, and reusability into the DNA of Bangladesh's digital governance. But vision must be matched with capacity, clarity, and sustainability. Without training, documentation, and oversight, the policy risks becoming symbolic rather than transformative. By learning from international experiences and adapting them to local realities, Bangladesh can turn "Public Money, Public Code" from a slogan into a civic contract. If implemented wisely, it can transform Bangladesh's digital infrastructure into a true national asset, serving not just the government, but the people whose money built it.