RIGHT SIGNAL TO PAK

Indian cricket team is not going to Pakistan for Champions trophy; kabbadi and blind cricket teams are also following the suit. This is a strong message sent across the border that we can't be playing cricket in the day and facing terrorism unleashed by Islamabad in Kashmir in the night. The Narendra Modi government must be credited with bringing absolute clarity in dealing with Pakistan, the sponsor of terrorism and delinking it from the task of sorting out the mess of seven decades in J&K. There is no longer facing terrorism in the day and then going to the Wagah border in the night to light candles for friendship. The point is unless you can identify a problem clearly, you can never think of its solution. The Modi government has made things very clear to Pakistan and unless you dismantle the terror infrastructure targeted at India and hand over the fugitives of the Indian law to Delhi, you will continue to face the indifference of India to your disadvantage. Also, the Modi government has made Pakistan pay the cost of its misadventures in India through its terror arm. Pakistan is a pauper state; it's marginalized in the global milieu and its leaders are begging for money not to restructure the country's economy but to repay the debts to avert default on payments. Terrorist leaders inside Pakistan are feeling unsafe. While on the other hand, there is peace and normalcy in J&K; development is in top gear and J&K is looking at a bright future despite occasional raising of head by the Pak-sponsored terrorists. The authorities and civil society is fighting the drug menace that came to Kashmir as part of the narco-terrorism cartel. The youth of J&K are being encouraged to travel, play sports for the country and attend colleges and universities for a good future while Pakistan is using its youth as cannon fodder in Kashmir.

Delhi discoms in crisis: Debt and regulatory gaps

Uttam Gupta

Delhi Government is looking at various options to address twin problems facing its three power distribution companies (discoms) namely BSES Rajdhani Power Limited (BRPL), discom for South & West Delhi; BSES Yamuna Power Limited (BYPL) — discom for Central & East Delhi; and Tata Power Delhi Distribution Limited or TPDDL - discom for North Delhi. These are (i) "Regulatory Assets" or RAs of Rs 27,200 crore lying in the books of these discoms; (ii) an equally staggering amount of Rs 26,500 crore they owe to power generation and transmission companies viz. Indraprastha Power Generation Co. Ltd (IPGCL), Pragati Power Corporation Limited (PPCL) and Delhi Transco Limited or DTL at the end of September 2024. The discoms are expected to sell electricity to the consumers at tariffs –duly approved by the Delhi Electricity Regulatory Commission (DERC) – that are set in a manner such that the revenue generated from sale at these tariffs fully cover the power purchase cost plus the cost of wheeling and distribution. The requirement is mandatory under the Electricity Act, of 2003. But, this is rarely complied with.

Under a highly convoluted regime, the tariff charged from households (HHs) consuming up to 200 units a month is Rs 3 per unit which is just about half of the average cost leading to an under-recovery of Rs 3 per unit. Including levies adding to 44.6 per cent, the shortfall comes to Rs 4.3 per unit (3x1.446). For HHs consuming between 201 and 400 units, the tariff is Rs 4.5 per unit implying an under-recovery of Rs 1.5 per unit. Including the levies, this comes to Rs 2.2 per unit. These under-recoveries are cross-subsidised by charging more from industries and businesses for which the tariff can go up to a high of Rs 16 per unit.

The irony is that despite charging exorbitant rates from industries and businesses, a good slice of under-recoveries from HHs consuming less than 400 units a month remains uncovered. Additionally, the Delhi government doesn't want the latter to even pay the small tariff of Rs 3 per unit (courtesy, of Kejriwal's freebies). Thus, discoms are told not to raise any bill on HHs consuming up to 200 units even as HHs consuming up to 400 units get a flat deduction of Rs 800 per month from the bill amount. Though the government promises to reimburse them for these subsidies from the state budget, this promise is held more in breach. This increases discoms' losses which are compounded by large-scale power theft.

Where do RAs fit in? RAs are created when state electricity regulatory commissions (in this case, DERC) accept that the tariffs don't cover discounts' purchase costs but don't raise rates. The gap between the cost and revenue generated from sales at tariffs (albeit unrevised) for supplied power, is booked by discom as receivable and classified as RA. This is contrary to the Electricity Act (2003) and the National Power Tariff Policy (NPTP) which says that "tariffs must reflect costs and regulatory assets should not be created". In December 2022, the Ministry of Power (MoP) even warned against creating a pile of RAs. But, all these regulations/warnings have fallen on deaf ears.

All losses incurred by discoms in Delhi during the last 11 years or so have been shown in their books as RAs. Regrettably, the RAs persist despite subsisting mechanisms to enable discoms to offset cost escalation by suitable increases in tariff. As per the order issued by MoP on November 9, 2021, discoms are allowed to impose a surcharge known as PPAC (Power Purchase Agreement Cost). Levied as a percentage of the 'total energy cost and fixed charge component' of the electricity bill, the surcharge is meant to compensate them for variations in the fuel and power procurement cost. Effective from July 2023, the DERC had last increased PPAC vide its order dated June 22, 2023, by 9.42 per cent for BYPL, 6.39 per cent for BRPL and 2 per cent for TPDDL. The current PPACs for these discoms are 31.6 per cent, 27.08 per cent and 33 per cent respectively. Moreover, DERC has allowed discoms to levy a surcharge of eight per cent.

This is intended to plug any shortfall in revenue vis-à-vis the cost still left unplugged after collection of PPAC. Despite these two impositions, the discoms continue to report a substantial shortfall in their revenue from the sale of electricity which is manifest in cumulative monumental RAs of Rs 27,200 crore. It is a manifestation of several glaring pitfalls: (i) the Delhi government isn't reimbursing discoms for the subsidies they give to target consumers on its behalf; (ii) large-scale power theft continues unabated; (iii) discoms have been submitting inflated bills/claims and other financial wrongs; (iv) inefficiencies get full protection. Hesitant to sanction tariff hikes against these extra/unjustified costs, DERC chooses the easy option of putting all these under RAs.

The idea of creating RAs is flawed. When, a discom petitions DERC to allow any cost increase in tariff, the latter can either reject or accept. In case of acceptance, it should take the process to its logical conclusion by sanctioning the requisite tariff hike and notifying it. It can't leave things hanging in the air by accepting but not 'approving' and 'notifying' the tariff hike. Unfortunately, this is what the DERC has been doing for over a decade. This has dangerous consequences.

First, once recorded in their books as RAs, discoms will leave no stone unturned in recovering the money say by getting sanction of a steep hike in tariff to make up for the entire cumulative deficit in revenue. Indeed, the matter had gone right up to the Supreme Court (SC) which in an order given in early 2023 had directed the DERC to let discoms recover their RAs. This could lead to a 100 per cent hike in tariff.

So, the regulator decided to contest that order. Second, until such time the requisite tariff hike is actually sanctioned by the DERC, the RAs can't be treated as an asset. Hence, there remains every possibility of the loans taken from banks and financial institutions (FIs) for funding them becoming non-performing assets (NPAs). Moreover, the banks/FIs may not give more to discoms and their suppliers namely IPGCL/PPCL/DTL more loans. Third, the discoms can leverage the ambiguous classification (neither outright rejection of a claim for tariff hike nor approval) to present claims to the DERC which the latter may not be willing to accept.

This leads to substantial claims getting bogged down in legal disputes at the appeal level or in higher courts. To conclude, providing for RAs in the books of discoms is a bad practice. Apart from discoms, it also puts the power generators and transmission companies at serious risk. It can impair the balance sheet of banks and FIs who have given loans to them.

It could mean a steep hike in tariffs on supplies to industries/businesses besides HHs consuming more than 400 units a month. To cap it all, it provides a 'cover up' for financial irregularities and corruption. The practice must be shunned.

As for the RAs already piled up, a thorough enquiry should be ordered to look into irregularities followed by recovery of money from those found guilty.

The discoms should be 'unshackled' from the controls of the State government. If the latter wants to subsidize or provide free power to certain consumers, the money should be given to them directly.

(The writer is a policy analyst; views are personal)

RATAN TATA: GIANT OF INDIAN INDUSTRY

Prof. (Retd. JU)
Verinder Singh Manhas

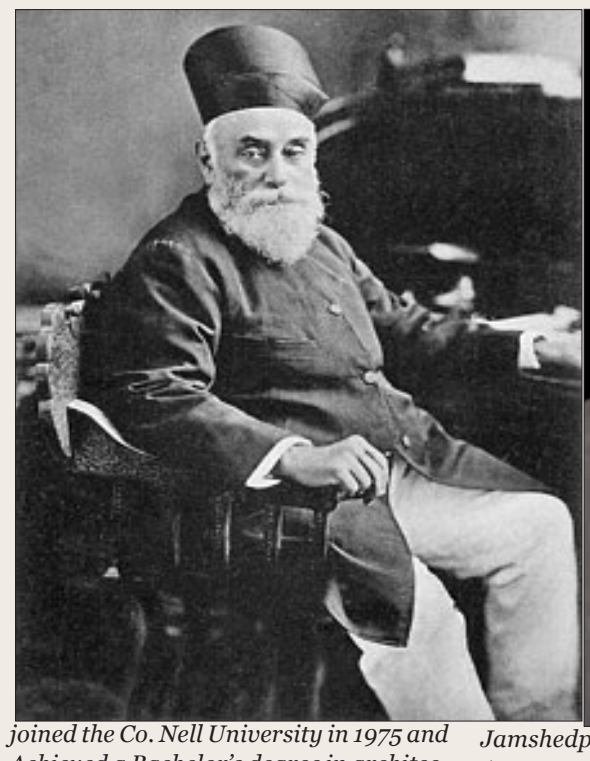
He came, He saw, He conquered, a quote true for Ratan Tata son of Jamshed Ratan Dadabhoy Tata a French Businessman, Philanthropist and aviator, who came to British India.

The Frenchman, Dadabhoy Tata was born in Paris, France on 28 December 1904 at Paris Lest (East) to his mother Suzanne Breire and Dadabhoy. Both were Parsi Zorastarians known for their wisdom and acumen. Jehangir Ratan Dadabhoy Tata was an honorary air marshal in French air force. He was awarded the highest civilian award' the legion of France in 1925 and appointed as director of French aviation manufacturing company at Toulouse in western France.

Dadabhoy migrated to India in 1935 and established the Tata Group comprising Tata Consultancy Services, Tata Motors, Voltas, Tata salt and Tata Airways (Air India).

He was assisted by his son Naval Tata establishing tata steels (Jamshedpur) Tata Batteries (Bhopal) Tata Engineering Services (Bangaluru). Rattan Tata was born in Mumbai in 1955 on 31 July.

Ratan Tata was the son of Naval Tata and the Grandson of Jamshedji Tata



joined the Co. Nell University in 1975 and Achieved a Bachelor's degree in architecture. Thereafter he joined the Harvard Business school and did advanced management in business in 1962.

He joined the Tata Group in 1962 after coming back from America his first engagement was with tata steels at Jamshedpur and tata tea with finlays in Assam.

In 1991 he succeeded Dadabhoy Ratan Tata as chairman of the tata group.

In his tenure, Ratan Tata expanded the Tata Group to Tata Tetleys, Tata Jagour and Tata Landrovers. The entire manufacturing of vehicles of Indian Army and Civil Trucks are manufactured by Tata Automobiles.

Ratan Tata breathed his last on 9 October 2024 at beach candy hospital in world, Mumbai was given a guard of honour and a 21gun salute by the state government of Maharashtra. A days mourning and holiday was declared in Maharashtra and Jharkhand

Besides the British knighthood in 2000, Ratan Tata was awardwd the order of Australia in 2023.

By his contributions to Tea Industry, Ratan Tata was awarded the Assam Baibhav in 2021.

Apart from these, he was awarded Padam Vibhushan in 2008, Maharashtra Bhushan in 2006, Padam Bhushan in 2009 and several other acclaides.

Among his successors are Cyrus Mistry and Natarajan Chandrashekaran.

He brought the industrial revolution to India whole heartedly by tata groups. He was a true follower of Satya Sri Sai Bana.

A Guide to Cyber Security Awareness for Students

Umesh Sharma

Cyber Security awareness is critically important among students as they are frequent users of digital technologies, yet often lack the knowledge or experience to recognize the risks they face online. With increasing amounts of personal and academic data being stored and shared online, students are prime targets for cyber criminals who exploit vulnerabilities such as weak passwords, unsecured networks, and social engineering tactics like phishing. As students, understanding the basic principles of cyber security is paramount to navigating this digital landscape safely. Cyber security awareness is more than just a nice-to-have skill for students; it's a necessary competence in our increasingly digital world. Recognizing the threats online and understanding how to protect yourself from them is critical for your safety, privacy, and overall digital well-being. Cyber security is not a destination but a journey that involves constant learning, adaptation, and vigilance. As a student navigating the digital landscape, your active participation in cyber security is crucial. Your decisions can make a significant difference in creating a safer online environment for yourself and your entire academic community.

As students continue to immerse themselves in the digital world, cyber security awareness becomes an essential skill. By educating students about potential risks and how to protect themselves online, educational institutions can help build a safer digital future. Ensuring that students are not only aware of the dangers but also equipped with the tools and knowledge to defend against cyber threats is crucial in today's technology-driven world. Ultimately, fostering a culture of cyber security among students doesn't just protect individuals-it helps to create a more secure and resilient digital environment for everyone.

The Role of Schools and Universities

Educational institutions have a significant role to play in promoting cyber security awareness. Many schools and universities have already begun to integrate cyber security lessons into their courses or offer workshops and seminars on the subject. Educational institutions, policymakers, and parents must work together to ensure students are equipped with the necessary skills and knowledge to navigate the online world safely. This includes integrating cyber security education into school curriculums, conducting awareness campaigns, and providing students with practical tips for maintaining their online security.

As student, taking proactive steps to boost your cyber security awareness is essential not only for protecting your personal information but also for contributing to a safer digital environment for everyone. In today's interconnected world, understanding the risks associated with online activities can help prevent cyber attacks, data breaches, and identity theft. Additionally, staying informed about the latest cyber security trends and sharing this knowledge with peers can help create a more security-conscious campus community, where everyone takes responsibility for safeguarding their digital presence.

Some tangible steps you can take as a student to boost your cyber security awareness and help create a safer digital environment:

" Stay Informed: Cyber security is dynamic, with new threats emerging regularly. Stay updated on the latest cyber threats and security practices by following reliable cyber security blogs, podcasts, or news outlets.

" Use Secure Connections: Whenever possible, avoid using public Wi-Fi for activities that require you to enter personal or sensitive information. If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to secure your connection.

" Regularly Update and Back up Your Data: Ensure your devices are constantly updated with the latest software versions, as these often contain security enhancements. Additionally, regularly backing up your data can help mitigate the damage if your device is compromised.

" Learn About and Implement Privacy Settings: Each social media platform and online service has different privacy settings and options. Take time to understand these settings and customize them according to your comfort level and needs.

" Enable Two Factor Authentication (2FA): Two factor authentication adds an extra layer protection on your accounts. Even when someone gets hold of your password, they won't be able to access your account without the second factor - usually a code sent to your phone.

" Strong Password Practices: Encouraging students to use complex passwords and change them regularly. They should also avoid using the same password across multiple accounts.

" Recognizing Phishing Attempts: Identify suspicious emails, messages, or websites that could be phishing attempts designed to steal sensitive information.

" Safe Use of Social Media: Helping students understand the risks of over sharing on social media platforms and the potential consequences of revealing too much personal information online.

" Downloading untrusted files: Additionally, students should be mindful of downloading files or software from untrusted sources, as these may contain malware.

" Participate in cyber security programmmes: Many schools and online platforms offer cyber security training. Participate in these pieces of training to deepen your understanding of cyber security and learn practical skills for staying safe online.

Cyber security awareness among students is no longer a luxury but a necessity in today's increasingly digital world. As students engage with technology daily for educational, social, and personal purposes, their vulnerability to cyber threats grows. The lack of adequate cyber security knowledge can lead to devastating consequences, such as identity theft, data breaches, or falling victim to scams and cyber bullying.

Moreover, fostering a culture of cyber security mindfulness helps students not only protect themselves but also contribute to a more secure digital ecosystem. By empowering students with the right tools and information, we can create a generation that is more resilient to cyber threats and more responsible in their digital interactions. Promoting cyber security awareness among students is essential for their safety and well-being. It is an investment in their future, enabling them to thrive in a digital landscape while safeguarding their privacy, security, and personal data.