Our Opinion, Their Opinion

"Do you want to know who you are? Don't ask. Act! Action will delineate and define you."
Thomas Jefferson

LS POLL TO BE FOUGHT ON CORRUPTION PLANK

The 2024 Lok Sabha election will be fought over corruption. This was made clear by Prime Minister Narendra Modi at a public rally on Sunday, the day when the Opposition attacked the Enforcement Directorate for arresting Delhi Chief Minister Arvind Kejriwal, some of his senior cabinet colleagues and the Jharkhand Chief Minister Hemant Soren. Calling the arrests a threat to democracy, the Opposition leaders said that the BJPled Central government has, therefore, to be ousted. The INDI Alliance partners met at Delhi's Ramlila Maidan to launch a verbal onslaught against the Bharatiya Janata Party and Prime Minister Narendra Modi at the "save democracy" rally. Modi promptly picked up the gauntlet. "They think Modi will be afraid...yeh Modi hai, jhukne wala nahi hai (This is Modi, he won't bend)," the prime minister warned. At the centre of the Opposition's attack was the Enforcement Directorate's crackdown on leaders of Aam Aadmi Party, the Congress, Trinamool Congress and other political parties in various states. The Prime Minister's sharp riposte turned the tables on the INDI Alliance partners as he said that his drive was against the corrupt and corruption while the Opposition wants to save the corrupt. Modi challenged them to attack him as much as they liked but warned that his crusade against corruption won't stop. Opposition's move to make Arvind Kejriwal and Hemant Soren's wives share the dais was done with the intention of earning voters' sympathy. It is doubtful if the move will succeed as voters have more trust in the prime minister's integrity than in any Opposition leader.

We still haven't figured out how to beat ISIS

Stripping ISIS of its self-proclaimed caliphate is not the same as beating it. By pulling back troops and intelligence assets from active conflict zones, the US has allowed groups like ISIS-K to rebound. It's not the time to let up, or we will find oursel

For all of the counter-terrorism wins that the United States has had in its fight against the Islamic State — and there have been many — we still have not figured out how to defeat it. A terrorist attack targeting a concert hall in the Russian capital of Moscow on March 22 killed more than 130 people and left many others severely wounded. It served as the latest deadly reminder that the Islamic State — and particularly its Khorasan branch, ISIS-K, which is active in Afghanistan, Iran and Pakistan — remains a potent threat.

It's a painful lesson Afghans and Americans alike learned in August 2021, when ISIS-K conducted a complex suicide operation that killed at least 170 Afghan civilians and 13 American service members in Kabul, in the midst of a chaotic US withdrawal from Afghanistan.

Since the start of the new year, ISIS-K has launched lethal assaults in Iran and Turkey. Several ISIS-K plots in Europe have been disrupted, with arrests in Austria, France, Germany and the Netherlands. On Tuesday, four days after the Moscow attack, the ISIS-affiliated al-Battar Media published a message threatening Italy, France, Spain and Britain: "Who's next?" Both France and Italy have since raised their terror threat levels.

All of these events point to what we now know: Stripping the Islamic State of its self-proclaimed caliphate is not the same as beating it. At its peak, the caliphate was as large as the territory of Britain, stretching from the Levant to Southeast Asia, and boasted over 40,000 foreign fighters from more than 80 countries. Forced from this redoubt, ISIS has reconstituted itself in other countries, going underground in less detectable — but more dangerous — forms.

To stop that threat from reaching America and its allies, the United States must prevent two decades of counter-terrorism expertise from atrophying. There are other serious threats that deserve Washington's attention, including Chinese adventurism and the challenge of artificial intelligence. But to keep Americans safe, counter-terrorism must remain a strategic priority — and that includes finding a way to keep eyes on the Islamic State in parts of the world where we no longer have a footprint.

After the terrorist attacks by Al Qaeda of Sept. 11, 2001, the American public was told to brace itself, that the war on terror would be a generational one. The United States made some profound blunders in the decades-long fight that followed, and eventually, Washington turned its national security focus to different geopolitical threats. But neither of those facts obviated the need to remain committed to countering transnational terrorism. By pulling back troops and intelligence assets from active conflict zones, the United States has allowed groups like ISIS-K to rebound. It's not the time to let up, or predictably, we will find ourselves facing a resurgent adversary.

The Islamic State is nothing if not resilient. Aggressive Western military campaigns helped dismantle the caliphate and have in recent years severely curtailed the operations of ISIS militants in other countries, including the Philippines and Syria. Rather than disappear, they have gone on to rebrand, enlist new fighters under the same banner and plot new attacks. Some have reappeared in other countries, better trained and harder to find and protect against. Some are intent on committing acts of terrorism like those we're witnessing now, traveling across borders to infiltrate target countries.

How did a jihadist group operating from a remote region of Afghanistan manage to expand its networks and begin planning external operations with such global reach?

Part of the answer is that we left. Before the United States withdrew, ISIS-K was far more constrained, particularly its ability to launch external attacks. In a 2020 agreement between the United States and the Taliban signed in Doha, Qatar, the Taliban agreed to prevent terrorist groups from using Afghan soil to threaten the United States and its allies. In return, Washington agreed to fully withdraw its forces from the country. The stipulation to prevent terrorist groups from using Afghanistan as an operating base was primarily relevant to the Taliban's longstanding, cozy relationship with Al Qaeda. The Taliban and ISIS-K, on the other hand, are mortal enemies and have been fighting each other since ISIS-K started operating in the country in 2015, at the apex of the Islamic State's so-called caliphate.

So while the Taliban, once in power, may have intended to combat ISIS-K and keep its militants in check, its success has been mixed at best. Taliban fighters were highly effective insurgents but are proving to be far less effective in their still new counter-insurgent and counter-terrorist role. They have made modest progress in eliminating ISIS-K commanders and reclaiming some territory from the group, but Islamic State militants still operate along Afghanistan's borders — and still retain the capacity for spectacular attacks.

Precisely because the Taliban has enjoyed some success in limiting ISIS-K's attacks within Afghanistan, the group has deliberately focused its energy on an "internationalisation" agenda, including shifting resources to build a robust external attack network. ISIS-K now maintains a vast network of extremists it can tap into, spread across volatile regions such as the Caucasus and Central Asia. Thousands of Central Asians have joined the Islamic State, with many Uzbeks and Tajiks holding leadership positions, especially in ISIS-K. Militants from Central Asia now form the backbone of ISIS-K's external operations cadre.

"In the past year, the Afghan affiliate has planned 21 external plots or attacks in nine countries, compared to eight plots or attacks in the previous year and just three between 2018 and March 2022," notes a report by the Washington Institute for Near East Policy.

Put simply: The Taliban is unable to contain the ISIS-K threat alone. The time has probably passed for trying to unseat the Taliban by discreetly supporting Afghan opposition groups like the Panjshiris of the National Resistance Front, who oppose Al Qaeda and the Taliban. Now it's time for diplomacy. Washington and its allies could engage the Qataris or the Saudis to provide incentives for the Taliban to ramp up their pressure on ISIS-K, share intelligence and, perhaps in time, walk away from their past pledge to unconditionally support Al Qaeda and provide the group with safe haven. Maybe the Taliban has learned from Mullah Omar's fateful refusal to hand Osama bin Laden over to the United States after the Sept. 11 attacks. Maybe not.

Security is no more a stand-alone function

The security of a democratic state includes the security of its citizens and today both are contingent on the wider security of the world at large. Similarly, at the level of an organisation its well-being is linked to the security situation within the country.

In the prevailing unsafe environment 'enterprise security' could no more be relegated to a set of hired 'guards' and security 'supervisors' since it has become a 'mainstream' function taking care of the organisation as a whole, including its members.

Rise of terrorism as an instrument of 'proxy war', targeting of economic lifelines of the country by the enemy and the advent of natural or man-made disasters on the national security agenda have all impacted on the security and safety of organisations -- big or small -- and put a new focus on the security management of corporate entities.

Terrorism basically is 'resort to covert violence for a perceived political cause' and since a 'cause' was driven by 'motivation' it was no surprise that faith-based driving force rooted in 'radicalisation' in the Islamic world with its advocacy of 'Jihad', had become the new terror threat globally.

Arising out of certain geopolitical developments traceable to 9/11 and the resultant 'war on terror' launched by the US, this danger faced nations across the world. India and its strategic establishments were particularly affected because of cross-border terrorism instigated by Pakistan against the country. In the post-Cold war era of 'proxy wars' there is also the added threat of enemy taking recourse to economically damaging the opponent in order to weaken the latter.

The need for economic security has in the process, added to the 'mainstreaming' of security function. Also,the importance of proactive measures required by organisations and individuals to deal with disasters, has further sharpened the role of the security set-up of the enterprise.

A deeper understanding of security of a business enterprise today calls for a conscious adoption of many practices that added upto the mainstreaming of security function. First, it should be understood that security is basically protection of the three assets of the organisation -- physical assets, manpower and protected information, against covert attacks of the enemy.

It clearly runs through the length and breadth of the enterprise correspondingly requiring 'physical', 'personnel' and 'information' security to prevent 'sabotage', 'subversion' and 'espionage' respectively. This makes security a mainstream function by the very nature of its mandate. In sensitive establishments of strategic importance personnel security is of overriding importance.

Apart from 'antecedent checks' at the time of recruitment, there has to be an internal 'vigilance' set up in place integrated with the 'security' function to detect signs of 'vulnerability' in an employee -- a member given to addiction, living beyond means or developing an unnatural and intimate friendship with an outsider of opposite gender, may have to be taken note of for reasons of security.

As regards security of information, it has to be protected first through 'classification' by way of giving the information a marking like 'restricted', 'confidential' or 'secret' and then determining the 'need to know' ambit within the organisation. Since most information is now on internet, a cyber security administrator under the IT Act is to be appointed and the security head would be a key functionary working with the latter. All of this makes security a very special function.

Security is an integral or complete looking concept requiring all its dimensions -- physical, personnel and information -- security related -- to be perfected. Further, security being a protection against the hidden attack of the unseen adversary, it is clearly anchored on information about the likely sources of threat that would have to be collated and analysed.

Most business corporates therefore had a central set-up for studying the market, evaluating the competitors and pooling together all reliable information relating to the three kinds of risks already mentioned. It produces what is called 'Business Intelligence' incorporating the 'risk assessment' for the enterprise. This means that the set-up has to be headed by a competent leader who had the skills of assessing what lay ahead in terms of both 'opportunity' as well as the potential 'risks'. This functionary has to be swift in handling information, capable of making assessments and confident about extending the outreach all the time.

Personal security of the leadership of an enterprise that made a substantial contribution to national economy is an important responsibility of this set-up in view of the recognised concept that a country's economic power strengthened its national security as well.

The second most important aspect of security is that it has to work on the authority of the top man of the enterprise. The chief of security has a matching knowledge of how various wings of the organisation were working. He should have the locus standi to take note of any flagrant violation of security even by a senior member of the organisation and for that reason alone should have a direct line of communication with the head of the enterprise. In fact, it is said that the top man should also consider himself as the head of security. Further, since security embraces all resources and members of the organisation it needs to be incorporated at the level of policy and should be one of the determinants of organisational ethics and in fact of the system of management of the enterprise itself. Also, since security does not come cheap it requires planned funding.

On his part the security chief should have the ability to realise that 'cost effective' security was the best security even when the organisation was liberal with funding. If two persons can do a job where three were deployed earlier or when the number of steps for completing an operation could be reduced from four to three, this makes the functioning more efficient and cuts delays.

Finally, the ultimate mainstreaming of security is reflected in the dictum -- now well established -- that the security of an organisation required contribution of all members, high or low in the hierarchy. It flows from the thought that if the enterprise ensured every member's security then the latter also owed it to oneself to do whatever was possible to strengthen the security of the organisation.

The importance of the security set-up being able to run 'awareness' programmes for the organisation as a whole suggests itself. This is best done through periodical informal 'briefings' that would also help to facilitate flow of information relevant to security from members to the security chief.

The security set-up has to be manned by people who were information savvy and professionally up-skilled. Such people can distinguish essentials from non-essentials in the context of security, know that 'you have to reach information -- information will not reach you', have curiosity which creates the 'spirit of inquiry', show an interest in human nature and behaviour and have an analytical mind.

The era of 'proxy wars' and the advent of cyber warfare have compelled the world to take note of the convergence of economic security, externally instigated attacks on systems on which the governance of the country rested and resort to 'misinformation' and 'deepfakes' even to influence the outcome of elections in a targeted country.

Artificial Intelligence is getting into security domain -- both in analysing the threats and finding solutions for dealing with them. Today, people handling enterprise security have to be familiar with various dimensions of knowledge economy and intricacies of misuse of cyber space by the adversary.

Security has become a demanding function linked to the mainstream of the organisation that was sought to be protected and dependent on people, who had special skills deserving of a higher level of recognition and compensation than what ever was existing earlier.

By-D.C. Pathak

When Gmail created a revolution in the world

Google co-founders Larry Page and Sergey Brin loved pulling pranks, so much so they began rolling outlandish ideas every April Fools' Day not long after starting their company more than a quarter century ago. One year, Google posted a job opening for a Copernicus research centre on the moon. Another year, the company said it planned to roll out a "scratch and sniff" feature on its search engine.

The jokes were so consistently over-the-top that people learned to laugh them off as another example of Google mischief. And that's why Page and Brin decided to unveil something no one would believe was possible 20 years ago on April Fools' Day.

It was Gmail, a free service boasting 1 gigabyte of storage per account, an amount that sounds almost pedestrian in an age of one-terabyte iPhones. But it sounded like a preposterous amount of email capacity back then, enough to store about 13,500 emails before running out of space compared to just 30 to 60 emails in the then-leading webmail services run by Yahoo and Microsoft. That translated into 250 to 500 times more email storage space.

Besides the quantum leap in storage, Gmail also came equipped with Google's search technology so users could quickly retrieve a tidbit from an old email, photo or other personal information stored on the service. It also automatically threaded together a string of communications about the same topic so everything flowed together as if it was a single conversation.

"The original pitch we put together was all about the three S's" — storage, search and speed," said former Google executive Marissa Mayer, who helped design Gmail and other company products before later becoming Yahoo's CEO.

It was such a mind-bending concept that shortly after The Associated Press published a story about Gmail late on the afternoon of April Fools' 2004, readers began calling and emailing to inform the news agency it had been duped by Google's pranksters.

"That was part of the charm, making a product that people won't believe is real. It kind of changed people's perceptions about the kinds of applications that were possible within a web browser," former Google engineer Paul Buchheit recalled during a recent AP interview about his efforts to build Gmail.

It took three years to do as part of a project called "Caribou" — a reference to a running gag in the Dilbert comic strip. "There was something sort of absurd about the name Caribou, it just made make me laugh," said Buchheit, the 23rd employee hired at a company that now employs more than 180,000 people.

The AP knew Google wasn't joking about Gmail because an AP reporter had been abruptly asked to come down from San Francisco to the company's Mountain View, California, headquarters to see something that would make the trip worthwhile.

After arriving at a still-developing corporate campus that would soon blossom into what became known as the "Googleplex," the AP reporter was ushered into a small office where Page was wearing an impish grin while sitting in front of his laptop computer.

Page, then just 31 years old, proceeded to show off Gmail's sleekly designed inbox and demonstrated how quickly it operated within Microsoft's now-retired Explorer web browser. And he pointed out there was no delete button featured in the main control window because it wouldn't be necessary, given Gmail had so much storage and could be so easily searched. "I think people are really going to like this," Page predicted.

As with so many other things, Page was right. Gmail now has an estimated 1.8 billion active accounts — each one now offering 15 gigabytes of free storage bundled with Google Photos and Google Drive. Even though that's 15 times more storage than Gmail initially offered, it's still not enough for many users who rarely see the need to purge their accounts, just as Google hoped. The digital hoarding of email, photos and other content is why Google, Apple and other companies now make money from selling additional storage capacity in their data centres. (In Google's case, it charges anywhere from USD 30 annually for 200 gigabytes of storage to USD 250 annually for 5 terabytes of storage). Gmail's existence is also why other free email services and the internal email accounts that employees use on their jobs offer far more storage than was fathomed 20 years ago. "We were trying to shift the way people had been thinking because people were working in this model of storage scarcity for so long that deleting became a default action," Buchheit said.Gmail was a game changer in several other ways while becoming the first building block in the expansion of Google's internet empire beyond its still-dominant search engine.

BY-MICHAEL LIEDTKE