India's Trishul
Casts Shadow Over Lashkar's Lahore Meet

Mili Muslim League (MML), known as the political wing of the proscribed Laskar-e-Taib (LeT) terror group from Pakistan, has indefinitely deferred its annual workers' convention, which is supposedly taking place at Minar-e-Pakistan in Lahore on November 2. Although a life threat to senior leaders of MML was cited for deferment, reports suggest that this decision was attributed to ongoing military tensions in the region, particularly India's Trishul operation.

The decision was taken by Hafiz Saeed, LeT's chief, and disseminated through informal meetings by senior leaders, not to make any public statements. Saeed was expected to personally address and lead the convention. The time of deferment and India's Trishul sparked controversies across the media.

Exercise Trishul is a tri-service exercise being carried out across multiple strategic locations, including the western front and the Arabian Sea. This exercise coordinated operations between the Army, Navy, and Air Force, incorporating multi-domain simulations and testing integrated warfare capabilities. The proximity of these operations to Pakistan's potential installations has triggered a heightened state military alert in Islamabad.

Pakistan has issued a second Notice to Airmen (NOTAM) within five days, reflecting the many effects are operation Trishul created in the region. The NOTAM is effective from November 1 to November 30, restricting access to a large portion of the country's airspace, particularly over the southern and coastal region. Intelligence reports indicate these measures are a byproduct of "panic and precaution" triggered by India's military posturing. Pakistan will also test live firing from November 2 to 5 in the Arabian Sea.

While some reports narrate that insiders within Lashkar expressed that the Trishul exercise may be one of the reasons for the convention's postponement, though the organization did not publicly admit that the deferment was linked to Trishul.

This development underscores the active security environment characterizing India-Pakistan relations, where military exercises and countersignals serve as a vehicle for strategic messaging between two nuclear-armed nations. The postponed Lashkar's convention exemplifies how tension between Indian and Pakistan has heightened.

Author: I.E.A

Border Violence Strains Pakistan–Afghanistan Ties

Fierce cross-border clashes this month have reignited hostilities between Pakistan and Afghanistan, exposing not only military tensions but also deeper geopolitical undercurrents in South and Central Asia.

In early October, Pakistan launched airstrikes in Afghanistan's Paktika and Khost provinces, claiming to target Tehrik-i-Taliban Pakistan (TTP) hideouts. Afghan authorities condemned the strikes as violations of sovereignty, reporting civilian deaths. Taliban forces retaliated by attacking Pakistani border posts, triggering days of heavy shelling across the frontier.

A ceasefire mediated by Qatar and Turkey on October 19 temporarily halted the fighting, but negotiations in Istanbul collapsed soon after. Pakistan's Defence Minister Khawaja Asif warned that Islamabad "will not hesitate to strike deep" if Kabul fails to dismantle militant sanctuaries.

Beyond the immediate violence, the standoff underscores Pakistan's growing frustration with the Taliban government it once backed. Islamabad now views Kabul's inaction on the TTP as a direct threat to national security, while Afghanistan accuses Pakistan of undermining its sovereignty.

Strategically, the conflict reflects a broader regional power struggle. China's expanding footprint in Afghanistan through mining and infrastructure projects, and Russia's renewed diplomatic engagement with Kabul, have complicated Pakistan's traditional leverage. At the same time, the U.S. and Gulf states are quietly watching, wary of renewed instability along a corridor linking Central and South Asia.

With trade routes blocked and trust eroded, the fragile ceasefire remains on edge. Analysts warn that if the two sides fail to align on counter-terrorism and border management, the crisis could reshape the regional balance and invite deeper foreign involvement.

Author: Shruti Kaushik

Historic Nuclear Policy Reversal
U.S. Resuming Its Nuclear Explosive Tests

A dramatic reversal in the American nuclear policy as President Donald Trump directed the Pentagon to start testing nuclear weapons immediately, ending the United States' 33-year moratorium on nuclear explosive testing. As usual, Trump made the announcement on Truth Social just hours before his scheduled meeting with Chinese President Xi Jinping in South Korea, stating that the test is necessary to march programs by Russia and China.

"Because of other countries testing programs, I have instructed the Department of War to start testing out Nuclear Weapons on an equal basis", Trump wrote. "That process will begin immediately".

U.S. nuclear testing moratorium is in place since 1992 after nuclear test "Divider" taken place at the Nevada Test Site. Initially, it was meant for nine months, however, then President Bill Clinton extended indefinitely, served as a cornerstone of international non-proliferation efforts. It doesn't mean the U.S. is not involving in nuclear programs, but it relied on computer simulations and laboratory techniques to maintain nuclear arsenal without explosive tests.

So why now? The resumption of nuclear explosive tests came amid escalating nuclear tensions with Russia which scrapped peace submit with Donal Trump.

President Vladimir Putin personally oversaw its strategic nuclear forces exercises and announced they had successfully tested its Poseidon nuclear-powered torpedo, a weapon that capable of devastating coastal regions through radioactive ocean swells.

Additionally, North Korea also tested its intercontinental ballistic missiles right before President Trump visiting South Korea where meeting with Chinese President Xi Jingpin scheduled to take place. Trump saying Russia is in second and China is third place in nuclear powered arsenal, however it will be even with Russia within five years. This exemplified how nations are engaging rapidly in developing nuclear arsenal. Trump also claimed the U.S. has more nuclear weapons than any other country, achieved through a complete update and renovation of existing weapons. He also mentioned that he hates tremendous destructive power, however, the action of other countries leaves no choice.

So far, the nuclear testing moratorium has positioned the U.S. to strongly advocate for the non-proliferation of nuclear weapons, especially countries like Iran, North Korea, and others. However, that credibility as leverage may no longer hold in future talks.

Author: I.E.A

The Devastating Civil War
and the Humanitarian Catastrophe in Sudan

While we are all raising our concerns over the Israel-Gaza conflicts, the civil war in Sudan is nearing its third year, registering one of the world's worst humanitarian crises and destabilizing the region. The conflict is happening between the Sudan Armed Forces (SAF), which is a military force, and the Rapid Support Forces (RSF), which is a strong paramilitary force of Sudan. In late October, the conflict escalated further as RSF captured the key city of el-Fasher in North Darfur. Reports suggest that this capture cost killing of at least 1500 civilians within 48 hours raises significant concern over civilian needs, grave fear of genocide and ethnic cleansing in the region.

This is not a mere military conflict but is a multipronged socio-political crisis rooted in Sudan's volatile governance, ethnic tensions, and competing visions of Sudan's future. RSF is a paramilitary force rooted in the infamous Janjaweed militias. It yields enormous influence and defies integration into regular armed forces. There are allegations of foreign support for RSF to keep the region destabilised. These factors clearly complicate the truce talks.

The ongoing power struggle is leaving its civilian population vulnerable to mass and targeted killing, sexual exploitation, and targeted destruction of medical facilities. The World Health Organization reported more than 460 patients were killed during attacks on healthcare institutions, underscoring the conflict's humanitarian toll.

More than 12 million Sudanese have reportedly been displaced internally or seek asylum in the neighbouring countries, making it one of the largest displacements in the world. Famine, starvation, and disease are widespread as humanitarian aids are blocked by ongoing conflicts. Even the UN and its aid agencies find difficulties in operation, reaching people in critical need, and increasing the risk of protracted humanitarian disaster. Countries like Germany, the UK, and Jordan have recently issued joint appeals for immediate humanitarian corridors and political dialogue.

Regionally, the Sudan conflict most likely fuels instability across the Horn of Africa and the Sahel region, with borders allowing armed groups and refugees to flow between countries. This influx poses a threat to neighbours who are already facing security threats and fragile governance.

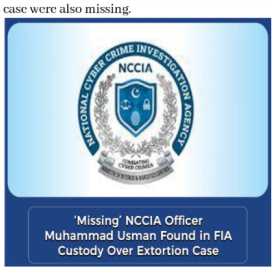
While nations raise their voice over Gaza and its humanitarian crises, Sudan is facing a multifaceted crisis whose implications reach far beyond its borders. The combination of political fragmentation, unstable governance, armed militia dominance, and international neglect creates a devastating situation for the civilians of Sudan who bear the violence, deprivation, and displacement. Urgent, coordinated international actions are needed to pressure the warring parties toward peace agreements, and such efforts could mitigate the risk of mass suffering, which is destabilizing the nation.

Author: I.E.A

Crisis Hits Pakistan's NCCIA
After Cybercrime Officers Reported Missing

A storm is brewing within Pakistan's security establishment as the country's premier cybercrime agency faces a crisis of disappearances, corruption, and institutional infighting. **The National Cyber Crime Investigation Agency (NCCIA)**, once introduced as a flagship body to fight digital crime, is now at the centre of a widening scandal involving missing officers and graft allegations that have exposed deep fractures across Pakistan's law enforcement and intelligence network.

On October 14, the wife of NCCIA Deputy Director **Muhammad Usman** filed a petition in the Islamabad High Court stating that her husband had been abducted by unidentified men from Islamabad. The court ordered the police to locate him within three days and warned senior officials of consequences if they failed. Usman was investigating a high-profile case involving YouTuber **Saadur Rehman**, known as *Ducky Bhai*, when he disappeared. During subsequent hearings, it emerged that several other officers associated with the same case were also missing.



'Missing' NCCIA Officer Muhammad Usman Found in FIA Custody Over Extortion Case

Within days, six NCCIA officers who had been untraceable for weeks resurfaced in the custody of the **Federal Investigation Agency (FIA).** They were produced before court on charges of bribery, misuse of authority, and extortion. An **FIR** registered against nine officials accused them of demanding Rs 9 million in bribes and diverting cryptocurrency worth over 300,000 dollars through Binance accounts linked to cyber fraud and online gambling networks.

In the aftermath, NCCIA Director General **Waqaruddin Syed** was transferred out of his position, and **Syed Khurram Ali** was appointed as his replacement. The development has reinforced suspicions of a deeper internal shake-up inside the agency.

The NCCIA had been carved out of the **Federal Investigation Agency's Cybercrime Wing** earlier this year to strengthen Pakistan's digital crime response. The initiative was initially hailed as a major step toward protecting national cyberspace. However, within months, the agency became mired in controversy as overlapping jurisdictions and alleged interference from intelligence outfits led to a collapse of coordination.

Staff shortages, corruption inquiries, and missing officers have now paralysed operations. The Islamabad High Court continues to press law enforcement for progress in locating Usman, while the FIA pursues graft charges against the officers in custody. So far, no government or intelligence body has issued a detailed statement on the matter, and the NCCIA has maintained silence apart from acknowledging that the situation is "serious."

Pakistan's cyber landscape is already volatile, with rising cases of crypto scams, financial fraud, and illegal betting networks siphoning billions of rupees through online channels. The NCCIA was expected to serve as the primary shield against these threats. Instead, it has become a symbol of institutional decay.

The case also highlights Pakistan's internal struggle for control over digital intelligence and surveillance. The creation of an independent civilian cyber agency had reduced the monopoly of traditional security institutions, sparking tension within the power structure. Now, with senior officers missing, arrested, or transferred, the balance of control appears to be shifting once again.

For the judiciary, the episode is another test of its ability to assert oversight over powerful institutions. The Islamabad High Court has granted the FIA a short physical remand of the accused officers while warning that failure to recover the missing deputy director would invite personal accountability for senior officials.

The crisis within the NCCIA is an isolated scandal. It reflects how corruption, political pressure, and unchecked power are eroding Pakistan's security architecture from within. At a time when cyber threats are becoming a front line of national defence, the country's own digital watchdog is collapsing under the weight of greed.

Author: Shruti Kaushik

Cross-Border Rohingya Militancy Resurfaces Along Arakan Coast

A maritime security incident on September 10, 2025, has heightened concerns regarding cross-border movements and the potential exploitation of fishing routes along the Bangladesh–Myanmar frontier. According to official sources from Myanmar, approximately 80 Bangladeshi fishing boats reportedly entered Arakan (Rakhine) waters around 1:00 PM, approximately 6.75 kilometers west of Koetankauk village and 6.72 kilometers west of Chainkharli village in Rathedaung Township.

While most of the vessels were allegedly engaged in fishing activity, Myanmar authorities stated that one of the boats carried armed individuals disguised as fishermen. During an attempted inspection by security personnel, the situation escalated, resulting in the deaths of one Arakan security officer and one coast guard member. The assailants reportedly fled toward Bangladeshi territorial waters after seizing their weapons.

Preliminary assessments by Myanmar's security agencies suggest possible links between the infiltrators and known Rohingya-based armed groups such as the Arakan Rohingya Salvation Army (ARSA) and the Rohingya Solidarity Organization (RSO). Both groups have been previously accused of cross-border militancy and involvement in transnational criminal networks operating in the coastal zones.

Authorities in Rakhine State have since increased maritime patrols and surveillance in coordination with coastal security forces to prevent further incursions. Myanmar's Ministry of Foreign Affairs is expected to raise the issue through diplomatic channels, emphasizing the need for stronger joint maritime monitoring mechanisms and intelligence sharing to prevent similar incidents.

Analysts note that while Bangladesh has consistently denied the presence of armed elements on its soil, the recurrence of such episodes underscores the importance of bilateral coordination to address overlapping security concerns, illegal fishing, and human movement along the porous maritime border.

Observers believe that sustained diplomatic engagement and cooperative security measures between Dhaka and Naypyidaw will be essential in maintaining regional stability, preventing the escalation of misunderstandings, and ensuring that extremist networks do not exploit humanitarian or economic vulnerabilities in the coastal region.

Author: Shruti Kaushik

Deepfake campaign targeting India's top officials

In the recent time, synthetic audio, images and videos created using Artificial Intelligence that simulate or fabricate contents, increasingly booming on the internet and quickly spread over social media, raises severe concerns in both social and legal aspect. It is commonly called deepfake contents. Once required powerful tools to create deepfake, now became a matter of single click by increasingly easy access to emergence of pocket friendly AI applications.

Deepfake is not mere a technological advancement but the sophistication, penetrating top government sector to daily entertainment. In the recent time, India's Press Information Bureau (PIB) Fact Check unit exposed coordinated campaign of AI-generated deepfake videos targeting country's top-officials with Pakistani propaganda accounts circulating manipulated content designed to undermine public trust in the government and military.

For instance, PIB flagged a digitally altered video of Indian President Droupadi Murmu featuring an artificial voice falsely claiming she was being "blackmailed" by the Prime Minister Narendra Modi's government to participate in rafale fighter jet promotional program.

The altered statement is "I want to request the citizens of our country that Modi Ji's Hindutva government blackmailed me and ordered me to sit in Rafale... If anything happens to me, Modi ji and his Hindutva politics will be responsible".

This is not the new but the latest in a series of AI-manipulated contents targeting Indian officials. Earlier this month similar AI-generated video where the finance minister Nirmala Sitharaman promoting fraudulent investment schemes promising returns of ₹60,000 in 24 hours and ₹10 lakh monthly.

It also falsely claiming minister promoting AI platforms like "QuantumAI" with unrealistic profit guarantees. Pakistan propaganda is not stopped there, circulated AI-generated videos of Home Minister Amit Shah falsely claiming he expressed desires for "saffronization" of Indian Army. Similar deepfake contents targeted lieutenant General Rajiv Ghai, Director General of Military Operations, with fabricated statements about "saffron politics" damaging military morale.

Why is it matter? Although deepfake could enhance entertainment and creativity, their potential for spreading false news demoralizing public and the government, undermining trust on the digital platform as they are evolving rapidly where the legislation hard to pick up.

Not everyone posses the capability or cognitive skills to identify the sophisticated deepfake contents. Hence, false propaganda could easily penetrate every corner of the world.

Reports suggest that many deepfake videos about the Indian Army are being run by foreign people's handles, and it is reported that Pakistan ISI could operate a dedicated cell to identify and recruit global influencers for spreading anti-India content, a part of broader information warfare campaign followed recent military operations.

For the raising concerns, while the PIB Fact Check continuously working for dismissing false claims targeted officials and shared reporting mechanism through WhatsApp or email, the Ministry of Information and Broadcasting announced plans to launch an AI-powered fact-checking chatbot and specialized software to detect deepfake contents.

Author: LEA

Don't Look Up

Billions of calls exposed via unencrypted satellites

Researchers from UC San Diego and the University of Maryland unveiled a shocking revelation, billions of global communications including phone calls, military secrets, and corporate data are being broadcast unencrypted through satellite networks, exposing sensitive information to any one with basic equipment costing as little as $600. It is to be considered one of a most comprehensive security breach in satellite communication to the date.

The study named "Don't Look Up" examined 39 geostationary satellites across 25 distinct longitudes using consumer-grade equipment which is usually available to any satellite television user. It is quiet shocking that how really our infrastructure relying on these satellite ecosystems believing it would all be encrypted. Whenever the team finds new, it comes unencrypted.

Intercepted data included thousands of T-Mobile user's phone calls and text messages during a nine-hour recording session, revealing communication from over 2,700 users. It also captures unencrypted internet communications from US military vessels, along with detailed Mexican military and law enforcement tracking data for helicopters, naval vessels, and armoured vehicles.

Beyond telecommunications, internal communications from major corporations and critical infrastructure been exposed. For instance, researchers intercepted inventory management data from Walmart, banking transactions from Mexican financial institutions, and operations communications from electric utilities and oil platforms.

People might assume no one would look these satellites and cross check what they have, and that's their method of security posing severe vulnerability. Many of the affected organizations are upgraded their security and implemented encryption fixes. However, some critical infrastructure operators have not implemented protection.

When the university researchers able to find these vulnerabilities, experts warn that intelligence agencies likely already exploit these vulnerabilities with their advanced equipment. India one among the nations that launches enormous satellites frequently, subjected to cyber-attacks very often.

India depends on satellites for critical tasks such as banking, utility monitoring, defence communications, law enforcement logistics and border surveillance increases national risk if traffic is unprotected.

It is learned that ISRO is working to develop and launch "hack-proof" satellites employing quantum communication technologies to further secure data in orbit. Additionally, government has already issued advisories and enforcement actions for encryption, secure API use, robust authentication, and continuous updates of satellite communications infrastructure. Although India's proactive measures suggesting increased awareness, the country remains exposed if older satellites, international data exchanges, or third-party providers have not met the latest encryption standards. Hence, vigilance and rapid security protocols are crucial for India's continued satellite infrastructure safety.

Author: LEA

"Jamaat-ul-Mominaat"

JeM (Jaish-e-Mohammed) women's wing

The JeM (Jaish-e-Mohammed) women's wing is named "Jamaat-ul-Mominaat." It was formed as the first-ever women's wing of the Pakistan-based terrorist group Jaish-e-Mohammed. The wing is led by Sadiya Azhar, the sister of JeM chief Masood Azhar. Recruitment for this wing began at Markaz Usman-o-Ali in Bahawalpur, Pakistan, and includes wives of commanders as well as economically vulnerable women from religious centres in various cities.

This development marks a significant shift in JeM's operational strategy, as traditionally, women were barred from armed or combat roles. The formation of the women's wing aims to train and use female operatives, potentially including female suicide bombers, in its terror activities. The group's leadership approved this move to counteract perceived threats and competition involving women on the opposing side, and to expand its influence through women, including via online networks in India.

The women's wing also offers indoctrination and training courses, like "Daura-e-Taskiya," mirroring the male training program and promising ideological rewards such as paradise for participants. Strict communication rules are imposed for members. This wing is part of JeM's broader efforts to rebuild following setbacks and to intensify its militant activities

The formation of Jaish-e-Mohammed's (JeM) women's wing, Jamaat-ul-Mominaat, represents a significant escalation in the group's threat to India, particularly in terms of operational and strategic capabilities.

Threat Overview

The women's wing is being trained and organized with the explicit goal of deploying female operatives in terror roles, including potential suicide missions and close-quarter attacks.

Leaders, including Masood Azhar, have publicly vowed that women who join the wing will be rewarded with paradise after death, framing their participation as both ideological and religiously sanctioned.

This development allows JeM to leverage societal vulnerabilities such as family networks and online recruitment channels, making it harder for security agencies to detect and intercept planned attacks.

Operational Implications

Female militants are less likely to attract suspicion, which increases the potential for covert urban attacks and espionage activities in India and neighbouring regions.

The wing includes a dedicated Fidayeen squad trained for suicide operations, expanding JeM's operational tactics beyond traditional male combatants.

The recruitment of women, particularly from families of slain militants or vulnerable social segments, exploits societal fissures and emotional connections, heightening the threat level.

Strategic Significance

This move signifies a tactical shift, aligning JeM's operational methods with other global terrorist organizations that have historically recruited women for combat and suicide missions, such as ISIS and Boko Haram.

The development complicates counter-terrorism efforts, as the presence of female militants presents new challenges in surveillance, intelligence gathering, and containment.

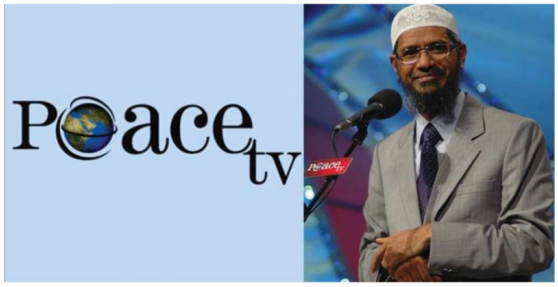
Vertical growth of the terror group's societal reach and the expansion of its ideological indoctrination suggest an increased threat not only in terms of immediate terror activities but also in galvanizing broader ideological support, which could inspire future recruits.

Conclusion

The emergence of JeM's women's wing is a clear indicator of the group's evolving threat landscape, enhancing its operational flexibility and expanding its capacity to carry out clandestine and high-impact attacks in India and the region. This development warrants increased vigilance and adaptive counter-terrorism measures by Indian security agencies.

Author: LEA

Bangladesh Welcomes Fugitive Zakir Naik



The relationship between India and Bangladesh is deteriorating day by day especially aftermath of ousting of former Prime Minister Sheikh Hasina and the emergence of Muhammad Yunus-led interim government at the center. In the latest dramatic policy reversal, Dhaka being ready to rollout red-carpet welcoming controversial Islamic preacher Zakir Naik, a fugitive in India for hate speech and terro-related charges.

The almost a month tour scheduled from November 28 to December 20, 2025, marking a significant shift in the Bangladesh diplomacy. Zakir Naik, once got banned following the July 2016 Holey Artisan Bakery terror attack in Dhaka where one of the bombers admitted that he got inspired by the speech of Zakir Naik. Shortly after the incident, Zakir Naik fled to Malaysia and residing there.

Indian agencies have flagged rising radicalization in Bangladesh under the current government, with concerns that Zakir Naik's visit could strengthen terror outfits like Harper-ul-Jihadi Islami (HuJI) and Jamaat-ul-Mujahideen Bangladesh (JMB), both designated as threats to India. Naik's visit is also viewed as a boost to anti-India activities, with connections suspected between him, Pakistan's ISI, and terror groups like Lashkar-e-Taiba and Jaish-e-Mohammad, who allegedly train Bangladesh-based militants to carry out strikes in India.

The Yunus government's decision to host Naik tells us one thing. Bangladesh is up for increased radicalization. During his visit, he is expected to deliver sermons across major cities, including madrasa and religious educational institutions, ike his last year visit to Pakistan, where he was photographed with key commanders of banned terrorist groups like Lashkar-e-Taiba.

Very recently, Muhammad Yunus has sparked tension with India by presenting a book titled "Art of Triumph: Bangladesh's New Dawn" to Pakistan's General Sahir Shamshad Mirza, during his visit to Dhaka. The book's cover depicted India's northeastern states, Tripura, Assam and oter region belongs to Bangladesh. This map appears to promote the "Greater Bangladesh" concept, a narrative that is being spread by radical Islamic groups like "ultanat-e-Bangla" which is backed by Turkish NGO. It extends Bangladesh borders into India's Northeast, West Bengal, and parts of Bihar, Jharkhand, Odisha, and Myanmar's Arkan region.

Additionally, there is a surge in radical Islamist groups in Bangladesh with incidents like campaign against ISKCON, demanding its ban accusing it of espionage for India and communal activities. Attacks on Hindu minorities also multiplied after Hasina ousted from the government. As diplomatic tensions escalated, the once-celebrated India-Bangladesh partnership rooted in shared liberation history and cultural ties, faces uncertain future. Bangladesh increased its engagement with Pakistan and China, by straining relations with India reflecting a broader realignment in Bangladesh's foreign policy under Yunus administration. These deliberate pivot against India's influence, raising concerns over national security and regional stability.

Author: LEA

Trump and his "Eight Wars Ended"?

Known for bombastic statements, President Donald Trump has been claiming that he has ended eight wars so far, that makes him deserves Nobel Peace Prize though it has been awarded to Venezuelan opponent party leader Maria Corina Machado for her continuous democratic work. With self-proclaimed title as the "President of Peace", Trump claims which ballooned from six in August to eight by mid-October coincides with high-profile diplomatic moves including fragile truce in Gaza and a fresh border agreement in Southeast Asia. Yet, many including fact-checkers and foreign policy analysts pointing out it as inflated and misleading, claiming that many conflicts are not being a war but skirmishes and violations. Let's have a closer look into those eight conflicts.

According to Trump's list, it spans the Middle East, South Asia, Africa, and beyond. The most recent one is peace deal brokered between Israel and Palestine in the early October, including hostage release and Israel's withdrawals. Trump addressed Israeli Knesset saying, *"This is not only the end of war, but end of the age of terror and death and the beginning of age of faith and hope"*. Though peace deal has been agreed, the conflict could erupt at anytime as Hamas being adamant on arms disarmament. Still reports from Gaza suggesting frequent ceasefire violation by both.

In June 2025, in the middle of exchange of missiles between Israel and Iran, U.S. strikes on Iran's key nuclear facilities, claiming it secure mutual ceasefire post-strikes. U.S. also claimed it neutralized Iran's nuclear escalations. However, Iran's denied all of Israel and U.S. claims that its nuclear facilities did not have adversarial impact as it safeguarded well. Violence could escalate anytime as if Iran restart its nuclear weapon programs.

Next, a four-day military escalation between India and Pakistan in May 2025, after Pakistan based terrorists killed 26 common people in Pahalgam which faced a strong stem response from Indian government, carried out Operation Sindoor, an endless war against terror, targeting key households of Pakistan based terror groups within Pakistan. Unsurprisingly, for defending terrorists, Pakistan retaliated with the help of equipment from Turkey and China. However, India alleged missile attack on the front of nuclear facility in Pakistan, driven ceasefire.

While Trump claimed he has brokered this

ceasefire with Pakistan embarrassingly obsequious to America, India denied it and said ceasefire has been initiated by only both parties' engagement. Hence, the credibility of Trump's claim has been under scrutiny.

In June 2025, Washington hosted representatives from both Democratic Republic of Congo and Rwanda, signed peace agreement. However, the M23 group which is main factor behind the decade long tension between both DRC and Rwanda, refused ceasefire as there were no representatives from M23. Later month, a permanent ceasefire brokered between M23 and DRC by Qatar, questioning the Trump claiming he has stopped the conflicts between DRC and Rwanda.

The border clash erupted between Thailand and Cambodia in July 2025 resulted in 35 deaths over disputed temple area. Trump threatened both countries with high tariffs if fighting is not stopped, and the truce came in effect as. Though, it has accomplished by economic leverage, in the very recent time, both counties agreed for the extended and comprehensive ceasefire once again in front of the Donald Trump.

The four decades of conflict between Armenia and Azerbaijan over a Nagorno-Karabakh, an ethnically Armenian enclave in Azerbaijan. It came to an end as both nations agreed to withdraw its forces, not involving forces from third countries and other conditions. The truce agreement was signed in the presence of Donald Trump at the Whitehouse. This is the only conflict that carries legitimate intervention by the United States.

Trump also claims he has stopped war between Ethiopia and Egypt as non-violent dispute over the Grand Ethiopian Renaissance Dam (GERD). In his first term, the U.S. helped to draft a potential agreement and later he claimed he "saved them from war" because Trump believed his involvement prevented Egypt from attacking Ethiopian Dam. But in reality, Ethiopia refused to sign the deal accusing U.S. being bias toward Egypt. Though no war was imminent, Trump used this episode for his peacemaker self-portrait.

In a similar incident, in 2020, Trump hosted leader from Serbia and Kosovo at the White House to sign a U.S.-brokered economic normalization deal which is focused on trade and infrastructure rather than political recognition, Trump, as usual, claimed this agreement has stopped the war, though, both countries were not at war at the time.

In overall, Trump's approach is blunt threats with deal-making, has yielded tangible paused in violence, particularly in Armenia-Azerbaijan and Thailand-Cambodia, and the White House deserves the credit for breakthrough. Meanwhile, the Gaza truce has seemed imperfect, but has saved lives and opened aid corridors, better than expected. However, the "eight war" claim is overrated and exaggerated noting the realities of conflicts where some weren't even violent or at the war.

Author: LEA

Google to invest $ 15B in India's largest A.I. Hub

In a historic landmark decision, Google announced its first huge $15 billion investment to build India's largest artificial intelligence hub particularly outside the United States. It is the biggest commitment to the South Asian nation amid rising trade tensions with Washington.

The project planned spanning over five years, establishing 1-gigawatt data centre campus in Visakhapatnam, Andhra Pradesh, integrating AI infrastructure with renewable energy capacity and international subsea cable connectivity. Google Cloud CEO Thomas Kurian described it as "the largest AI hub that we are going to be investing in anywhere in the world outside of the United States'.

The announcement comes as US-India relation face strain from President Trump's 50% tariffs on Indian imports imposed in August, prompting Prime Minister Narendra Modi to promote "made in India" products more rigorously. For instance, the recent local alternatives including Zoho Corporation's services competing with Google Workspace and Gmail, WhatsApp-rival Arattai, and MapMyIndia as a Google Maps alternative.

Despite this push for digital independence, Google's massive investment epitomizes India continued thriving for being a technology hub.

The project has been backed from key officials including Finance Minister Nirmala Sitharaman and IT Minister Ashwini Vaishnaw called it "a very important contribution to the India AI mission goals".

This upcoming facility will feature Google's complete AI technology stack, including custom Tensor Processing Units and access to Gemini AI models. It will also support consumer services like Google Search, YouTube, Gmail, and Google Ads while serving as a testbed for AI research across India. This project partnered with Indian telecom giant Bharti Airtel and AdaniConneX, a subsidiary of Adani Group for infrastructure development. It is expected to create over 1,00,000 jobs and would generate approximately $15 billion in U.S. GDP through AI and cloud services between 2026 and 2030.

The Google's investment in Visakhapatnam, positions India as a global connectivity hub through new international subsea cables, complementing existing gateways in Mumbai and Chennai. Overall, this infrastructure will enhance India's digital resilience while supporting government's ambitious target of 6 gigawatts of data center capacity by 2029.

Author: LEA

India Deepens Trade Ties with MERCOSUR

As global commerce faces mounting protectionist pressures, India and Brazil announced a landmark decision to potentially expanding the India-MERCOSUR Preferential Trade Agreement.

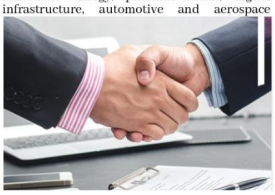
Understanding the MERCOSUR-India Trade Framework

MERCOSUR, the Southern Common Market is the premier South American trade bloc, member countries including Brazil, Argentina, Paraguay, Uruguay, and Bolivia. India signed a Framework Agreement with MERCOSUR in 2003 and Preferential Trade Agreement in 2004 which became fully operational since 2009. Unlike comprehensive free trade agreements that eliminate tariffs across most sectors, the current PTA covers only 450 tariff lines with preferential duties ranging from 10 to 100 percent reduction on selected products. In fiscal year 2024-25, India's exports to MERCOSUR accounted for USD 8.12 billion while imports stood at USD 9.36 billion, primarily from Brazil. Indian exports under the PTA include pharmaceuticals, chemicals, textiles, leather goods, machinery, and automotive components, while MERCOSUR sends food preparations, organic chemicals, essential oils, plastics, and rubber products to India.

Recent expansion

Brazilian Vice President Geraldo Alckmin visited New Delhi in October 2025, both nations agreed to expand PTA's coverage to include tariff and non-tariff issues across thousands of product lines. The two countries established technical dialogue through the Joint Administration Committee to define its scope and modalities. Brazin expressed confidence in concluding negotiations within ten months.

The aim of expanded PTA is to increase India-Brazil bilateral trade from $12.2 billion to $20 billion by 2030. Apart from tariff reduction, this agreement facilitates investment flow in renewable energy, pharmaceuticals, digital infrastructure, automotive and aerospace



industries, semiconductors, and advanced manufacturing. Brazil proposed launching a bilateral Digital Partnership focusing on AI, high-performance computing, and technology startups to green growth and innovation.

Strategic Implications

The MERCOSUR-India expansion aligns with key member of BRICS alongside Brazil, India deepening ties with Latin America bloc, home to over 300 million consumers provides market diversification amid global trade tensions especially absurd tariff by the United States.

This Southern Common Market agreement will enhance market access for Indian products, reducing reliance on Chinese and European suppliers. Agricultural exports from MERCOSUR including soybeans, food preparations, and raw materials complement's India's strength in pharmaceuticals, IT services, engineering goods and textiles.

The consensus between South Asia and Latin America could enhance resilience against disruptions affecting global commerce. The partnership strengthens India's multipolar foreign trade strategy by complementing ongoing FTA negotiations with the European Union, United Kingdom, and Indo-Pacific partners. From a geopolitical perspective, deepening India-MERCOSUR ties reinforces South-South cooperation frameworks the promote equitable global development outside traditional North-South aid relations. India-Brazil being as emerging markets collectively navigate trade tensions, regional bloc like MERCOSUR provides alternative growth pathways that is less vulnerable to western tariff fluctuations.

Although it is promising, there are few significant obstacles as Agricultural protectionism remains contentious with MERCOSUR countries especially Brazil and Argentina maintaining strong protection for their agricultural sectors limiting Indian access for products like sugar, pulses, and diary. Unlike FTA, MARCOSUR operates as a custom union requiring consensus from all its members, potentially slowing decision-making. Additionally, infrastructure and logistics between Indian and South America including transportation costs, shipping inefficiencies and supply chain gaps can limit trade flows.

Overall, as global trade architecture fragments amid rising protectionism and geopolitical tensions, the India-MERCOSUR expansion represents a pragmatic response that prioritizes South-South cooperation, market diversification, and regional value chain development. Although challenges remain substantial, the partnership offers both sides with opportunities to reduce vulnerability to Western tariff shocks and position themselves as leader in an increasingly multipolar economic order.

Author: LEA

Strength Beyond War

The war between Russia and Ukraine has entered a critical phase marked not only by fierce combat but by deliberate attacks on infrastructure, energy, and supply chains. In the past ten days, the scope of the conflict has expanded beyond the battlefield into a test of national resilience and strategic endurance.

In Washington, fresh sanctions on Russia's oil giants like Rosneft and Lukoil have reverberated across global trading networks. China, responding to those measures, suspended seaborne imports of Russian crude, while the European Union tightened restrictions on Russia's shadow fleet and curtailed the movement of its diplomats across Europe. Meanwhile, a planned summit between U.S. President Donald Trump and Russian President Vladimir Putin in Budapest was cancelled, following Trump's meeting with Ukrainian President Volodymyr Zelenskyy, during which Kyiv's request for Tomahawk cruise missiles was declined in favour of urging territorial concessions to pursue peace.

Even as diplomatic options narrow, Ukraine has moved decisively to strike deep inside Russian territory. In a significant escalation this week, the Ukrainian Navy launched Neptune missiles against Russian energy infrastructure, targeting key oil depots and logistics hubs that support Moscow's war operations. These precision attacks, carried out deep within enemy territory, signal a shift in Kyiv's strategy from defensive endurance to calculated retaliation. The strikes disrupted Russian supply routes in the Black Sea region and underscored Ukraine's growing technological and tactical sophistication despite limited resources.

Russia's actions have carried serious global implications. By weaponising energy flows and intensifying strikes on civilian infrastructure, Moscow disrupted European energy markets, triggered inflationary waves in import-dependent countries, and forced nations to reconsider their reliance on imported fuel and single supply routes. The bombardment of Ukraine's power grid and logistics hubs has caused humanitarian distress and exposed vulnerabilities in modern supply systems.

Amid this disruptive environment, Ukraine's survival strategy offers a master class in national resilience. Faced with a stronger adversary, Kyiv has embraced a multi-pronged approach: maintaining essential exports, investing in energy diversification, decentralising industry and digital capacity, and fostering community-level adaptive governance.

Agricultural exports, long a backbone of Ukraine's economy, continue to flow through alternate corridors along the Danube and by rail via Poland and Romania. Tech firms and startups have shifted operations westward or into neighbouring countries to sustain work and foreign contracts. The rapid deployment of localised renewable energy projects and micro-grids provides redundancy when the main grid is hit. At the community level, volunteer networks, local cooperatives and municipal repair teams step in when national infrastructure is challenged.

For India it's a must learn where strategic shocks are accelerating norms, the path to true self-reliance lies in thoughtful resilience. Few key focus areas:

Energy: Diversify sources, rapidly scale wind and solar with storage, build micro-grids for critical hubs, and expand strategic fuel reserves and alternate import routes.

Food & Logistics: Decentralise storage of essential commodities, strengthen inland waterway and rail connectivity to reduce dependency on single export / import corridors.

Industry & Supply Chains: Encourage modular manufacturing and flexible production facilities, develop domestic capability for critical components currently dependent on external suppliers.

Digital & Cyber Resilience: Distribute data infrastructure geographically, establish rapid recovery units for essential services, and build sovereign cloud and backup systems.

Local Governance & Civil Preparedness: Empower communities with emergency repair squads, ensure continuity of schooling, administration and utilities under disruption, and foster civic networks prepared for rapid response.

Diplomacy & Economic Hedging: Maintain diversified partnerships, enshrine contingency mechanisms for trade and insurance shocks, and avoid overreliance on any one power or route for strategic supply.

Reconstruction as Transformation: Attach every rebuilding project to green standards, invest in vocational training for sectors such as renewable installation and digital repair, and use crisis as opportunity to leap into a more resilient future.

This war shows, survival is not accidental. It is the outcome of deliberate planning, swift adaptation and societal cohesion. Ukraine's capacity to withstand sustained pressure and emerge not just functioning but future-oriented is a powerful example. For India its a learning that safeguarding the nation demands more than defence and diplomacy, it demands building a society and economy that can withstand shock, adapt quickly and keep moving forward. In a world defined by uncertainty, resilience must become the new normal.

Author: Shruti Kaushik

WTC Command Hubs Multiply as China Militarises the Plateau

Massive Chinese military buildup seen at Lhunze, Golmud and Pangong Tso as PLA fortifies Tibet and Qinghai sectors

Beijing's high-altitude military buildup has entered a decisive new phase. Fresh satellite imagery reveals sweeping upgrades at multiple People's Liberation Army (PLA) facilities along the Indian border, part of a broader effort to consolidate China's air, missile and air-defence network across the Tibetan Plateau.

At **Lhunze Airbase**, located about 100 kilometres from India's Tawang sector, construction of **36 new hardened aircraft and helicopter shelters** has been confirmed. The expansion, visible since April, transforms what was once a limited logistics post into a combat-ready forward base. Defence officials note that Lhunze and nearby Nyingchi have long served as corps-level supply depots. The new shelters, runway work and support buildings indicate a shift towards sustained air operations. Nyingchi now anchors a ten-kilometre belt of storage facilities linked to the Lhasa-Nyingchi expressway and the railway line extending into Sichuan, forming an integrated military corridor through the mountains.

The upgraded infrastructure gives the PLA the ability to launch and recover aircraft within minutes of India's northeastern defences, reducing reaction time and complicating Indian Air Force operations in the eastern sector.

Further north, **new missile construction near Golmud city in Qinghai Province** marks the most significant westward push of the PLA Rocket Force in recent years. Satellite analysis shows a large complex with launch pads, garages for transporter-erector-launchers (TELs) and camouflaged dome structures used to conceal movement. The facility, situated at high altitude on the Qinghai-Tibet Plateau, appears designed for road-mobile missile units consistent with PLA Rocket Force operations.Analysts believe the Golmud complex may fall under **Base 64 at Lanzhou**, with possible links to the **647th Missile Brigade** based in Xining, which operates **DF-26 intermediate-range ballistic missiles** capable of striking targets up to 4,000 kilometres away. The DF-26 can carry both conventional and nuclear warheads, giving Beijing a dual-capable deterrent that can reach deep into India's interior as well as allied facilities across the Indian Ocean region.

The new complex extends China's strike envelope westward, offering greater strategic depth beyond the reach of India's missile systems. It also reflects Beijing's continuing modernization drive. By 2024, the US Department of Defense estimated China possessed about 250 DF-26 launchers and was moving rapidly towards 1,000 nuclear warheads by 2030.

Field exercises by Rocket Force units in Qinghai, Gansu and Xinjiang throughout 2024 suggest that Golmud is already active. Reports of high-altitude training, new launch tests and the movement of TEL vehicles confirm that western China has become a key zone in the PLA's evolving deterrence posture.

Closer to the Line of Actual Control, a third development highlights Beijing's determination to secure its forward positions. On the **eastern banks of Pangong Tso Lake in Tibet**, about 110 kilometres from one of the 2020 clash sites, satellite images have identified a **new Chinese air-defence complex.** The facility features command posts, radar sites, vehicle sheds and a series of **covered missile-launch bays** with retractable roofs allowing Transporter- Erector-Launcher vehicles to remain hidden until launch.

Defence analysts assess that the site likely houses the **HQ-9 long-range surface-to-air missile system,** a core element of China's integrated air-defence network. A nearly identical complex has been spotted at Gar County, about 65 kilometres from the Line of Actual Control and opposite India's expanded Nyoma airfield in Ladakh. Such hardened missile positions, commonly seen in the South China Sea, are a new feature on the Himalayan frontier.

Each of these developments, from the fortified Lhunze airbase to the Golmud missile hub and the Pangong air-defence site, points to a clear strategic pattern. China is embedding permanent and survivable military infrastructure in Tibet and Qinghai, capable of sustaining both air and missile operations under contested conditions.

For India, the implications are immediate. The Chinese buildup compresses warning times, erodes the buffer once provided by terrain and introduces new risks of escalation during any border confrontation. New Delhi has strengthened its own forward bases and missile deployments, but the pace of Beijing's expansion indicates a sustained and long-term posture shift rather than a temporary show of force.

The Himalayas are no longer a geographic barrier. They are being engineered into a launchpad.

Author: Shruti Kaushik

PLA's Light Brigades with SWS3 Air Defense Systems to Counter Drone Threats

The People's Liberation Army (PLA) has officially inducted the new SWS3 short-range air defense system, also designated as the LD35L, into its light combined arms brigades, marking a significant step in strengthening the force's capability against modern aerial threats.

The SWS3 system integrates a 35mm autocannon with FB-10A short-range surface-to-air missiles, mounted on a highly mobile Dongfeng Mengshi 6×6 wheeled chassis. This configuration provides dual-layered protection, combining rapid-fire kinetic interception with missile-based precision engagement. The system is designed to detect, track, and neutralize low-altitude targets such as unmanned aerial vehicles (UAVs), loitering munitions, and cruise missiles, threats that have become increasingly common in modern battlefields.

Light combined arms brigades are among the PLA's most agile and modular formations, structured for rapid deployment and high mobility across diverse terrains. These brigades typically spearhead reconnaissance, flanking, and area-denial missions, often operating ahead of heavier mechanized or armored forces. Their operational design emphasizes independence, allowing them to function effectively in dispersed combat environments with limited centralized support.

Until recently, such brigades relied primarily on man-portable air defense systems (MANPADS) or on-cover fire from larger formations.

The introduction of the SWS3 provides them with an organic short-range air defense (SHORAD) capability, integrated directly into their maneuver elements. This significantly enhances their survivability against aerial reconnaissance and drone attacks.

The system's mobility allows light brigades to maintain protection during rapid advances or relocations, a capability the PLA has sought to refine as part of its ongoing modernization drive. The SWS3 also complements the PLA's emphasis on electronic warfare resilience and decentralized command, ensuring that forward-deployed units retain autonomous defensive capability even under disrupted communication conditions.

By integrating the SWS3 into its light brigade structure, the PLA is reinforcing its doctrine of layered air defense and operational self-sufficiency. The move signals China's recognition that low-altitude threats, particularly drones and precision-guided munitions, now represent a primary challenge in both conventional and gray-zone warfare environments.

Analysts view this induction as another step in the PLA's transition toward networked, mobile, and adaptive combat units capable of independent operations in contested airspace.

Author: Shruti Kaushik

China's Cyber Offensive Scales Up

China's cyber operations are entering a phase of accelerated integration, a coordinated push that fuses intelligence, administrative, and military objectives into a single digital command structure. The recent breach attempt by the Chinese-linked hacker group ***Salt Typhoon*** on a major European communications provider on October 19, 2025, underscores a growing convergence between Beijing's cyber-espionage apparatus and its strategic doctrine.

The attack exploited vulnerabilities in *Citrix NetScaler Gateway,* a software widely used for secure remote access, marking another escalation in China's digital penetration tactics. The episode is not an isolated intrusion; it represents the latest phase of Beijing's long-term playbook, refining techniques in peripheral theatres before applying them to high-value Western targets.

For the Chinese Communist Party (CCP), Southeast Asia has become the perfect "low-friction" cyber laboratory, a region where operations can be executed with limited political backlash. Governments in ASEAN, wary of jeopardizing trade or investment ties with Beijing, often avoid public disclosures of cyber intrusions. This reluctance has provided China's cyber units a permissive environment to test new tools and tactics, from VPN exploitation and router hijacking to bypassing lawful interception systems.

Historical patterns reveal the intent. Earlier campaigns like *Operation Soft Cell* and *APT40's maritime espionage* between 2018 and 2020 were meticulously designed to refine methods that would later be redeployed against critical infrastructure in the West. Southeast Asia thus serves as a proving ground where the boundaries between espionage, sabotage, and strategic positioning blur.

Western intelligence agencies tend to categorize China's Advanced Persistent Threats (APTs) by sectoral focus, such as military, telecom, or operational technologies. However, this compartmentalized view misses the underlying architecture: Beijing's cyber units are not isolated entities but extensions of a centralized national strategy. The CCP has dissolved bureaucratic barriers between digital operations arms, from the Ministry of State Security (MSS) to military cyber divisions, allowing unified direction under a national cyber command structure.

This integrated model ensures seamless transitions between espionage and disruption. The objective is not limited to information theft; it extends to "Day One" sabotage capabilities, the ability to paralyze communication networks, logistics systems, and energy grids at the onset of a geopolitical crisis. In a Taiwan contingency, synchronized cyberattacks could cripple regional telecom, disable transportation controls, and lock hospital databases, eroding an adversary's military readiness before the first missile launch.

The Salt Typhoon operation traces its sophistication to years of reconnaissance in ASEAN states. Since 2019, the group has targeted ministries and telecom providers across Southeast Asia, building operational familiarity with regional digital ecosystems. Vietnamese officials had warned as early as 2018 about the proliferation of "dangerous code transfers," a subtle reference to coordinated cyber intrusions, warnings that were largely disregarded by Western capitals.

APT40's maritime espionage in Malaysia, which preceded *Volt Typhoon's* high-profile attacks on U.S. ports and logistics facilities, further illustrates the methodical progression of these threat vectors. Each campaign refines tools and tradecraft, transforming Southeast Asia into a live testbed for global operations.

When breaches such as *Salt Typhoon* are exposed, the corporate victims often face regulatory scrutiny rather than systemic support, reinforcing underreporting and enabling China's asymmetric advantage. This silence benefits the attacker, shielding its methods from countermeasures while eroding public trust in corporate cybersecurity frameworks.

The economic implications are already significant. Estimates suggest that *Salt Typhoon* alone inflicted over $15 billion in cumulative damage across Western industries. Yet, recent U.S. engagements indicate a strategic recalibration. The 2024 CISA : Vietnam Memorandum of Understanding and the Philippines' Enhanced Defense Cooperation Agreement (EDCA) are emerging as pivotal mechanisms for coordinated cyber resilience. Together, they can transform U.S. Indo-Pacific Command (INDOPACOM) from a reactive defense posture into a proactive deterrence hub.

In essence, China's cyber operations represent a continuum rather than sporadic acts of aggression. The CCP's approach treats cyberspace as both a domain of warfare and an instrument of political influence. By leveraging Southeast Asia as a strategic rehearsal zone, Beijing is building a multi-layered capability that blends surveillance, disruption, and strategic coercion.

The challenge for the international community, particularly Indo-Pacific stakeholders, lies in recognizing these operations not merely as espionage, but as pre-emptive conditioning for future geopolitical conflicts. Before the next breach transitions from experimental to operational, regional actors must determine whether their digital infrastructure is ready for the scale and precision of the threat now taking shape.

Author: Shruti Kaushik