India's Human Touch in Ukraine's Crisis

Defense and Humanitarian Aid as Crisis Enters Fourth Year

In a significant shift from its earlier stance of strategic neutrality, India has expanded its assistance to Ukraine, providing crucial defense equipment and humanitarian aid as the Eastern European nation continues to defend itself in the ongoing conflict.

Sources close to the Ministry of External Affairs confirm that India delivered a package of military and medical supplies to Kyiv last month, including defensive equipment, medicines, and essential humanitarian goods. This marks the third such delivery since late 2024, representing an evolution in India's approach to the crisis.

India's principled support for Ukraine demonstrates that the world's largest democracy charts its humanitarian course with an unwavering moral compass, undeterred by geopolitical pressures from global powers like Russia or the United States.

The aid comes as India balances its historic ties with Russia against growing partnership with Western nations. Analysts suggest this calibrated approach allows India to maintain diplomatic channels with both sides while emphasizing its commitment to humanitarian principles.

Ukrainian Ambassador to India Oleksandr Polishchuk expressed gratitude for the assistance, noting that "India's support demonstrates

its emerging role as a responsible global power committed to international peace and stability."

Beyond government channels, Indian pharmaceutical companies have ramped up production of critical medicines for Ukrainian hospitals, while Indian NGOs have established rehabilitation centers for Ukrainian civilians affected by the conflict.

India's technical expertise has also been deployed, with IT specialists helping Ukraine strengthen its cyber defenses and agricultural experts providing consultation on food security measures.

As the morning sun rises over both New Delhi and Kyiv, separated by thousands of miles yet connected by threads of compassion, India's actions remind the world that true strength lies not just in military might or economic power, but in the courage to extend a helping hand across continents. In this global moment of darkness, it is these acts of human solidarity that illuminate the path toward a more peaceful tomorrow.

Western Theater Command

China's Hollow Logistic Support

China's Western Theater Command (WTC) projects an image of technological sophistication and logistical excellence while concealing significant vulnerabilities and human costs.

Following President Xi Jinping's high-profile Tibet visit in late 2024, Lieutenant General Zhao Zongqi took command of the Joint Logistics Support Force. Xi's push for self-sufficient military supply chains diverts resources from pressing socioeconomic needs, serving both as tactical initiative and propaganda tool.

The WTC's much-touted technological systems—quantum communications, AI networks, and drone fleets—frequently malfunction behind the scenes. Engineers face immense pressure to report success regardless of actual performance, creating dangerous capability gaps unknown to leadership.

In WTC's forward logistics hubs along contested borders, soldiers endure harsh conditions while maintaining a façade of readiness. During exercises like

Western Transport-2024, units stage elaborates performances where fuel trucks run empty with manipulated gauges and medical supplies are temporarily borrowed from civilian facilities.

The infrastructure supporting WTC operations comes at tremendous human cost. Construction crews work in extreme conditions with inadequate safety measures on strategic railways and highways cutting through the Tibetan plateau.

Meanwhile, local laborers near facilities like the Lhasa supply depot work extended shifts in sub-zero temperatures within a system that leverages access to housing and education to ensure compliance.

The military's resource prioritization creates economic distortions across the region. Factories shift from producing essential civilian goods to manufacturing military components, often at financial losses subsidized by debt-burdened local governments.

The Fragility of Force

China's Western Theater Command logistics system ultimately rests not on technology or infrastructure but on people. People increasingly caught between impossible demands and human limitations. The facade of strength requires continuous effort to maintain, consuming the very resources it aims to project. Within this system lie the seeds of vulnerability, as those who bear its weight begin questioning its purpose and sustainability.

As pressure mounts on those maintaining this complex illusion, small acts of resistance multiply data subtly altered, resources quietly redirected, information selectively shared. Together, these human responses to an inhuman system may ultimately determine whether China's logistical house of cards stands or falls. The true strength of any military system lies not in its appearance but in the willing participation of those who operate it—a factor increasingly in question across the Western Theater Command.

KALADAN PROJECT STALLED AS REBELS HOLD KEY TOWN

India's $430 million gamble locked in rebel territory

India's ambitious Kaladan Multi-Modal Transit Project faces an uncertain future 14 months after *Myanmar's Arakan Army (AA)* seized control of Paletwa, a crucial junction town in Chin State near the Bangladesh border.

The $430 million infrastructure initiative, designed to connect India's northeastern states to the Bay of Bengal via Myanmar, has been effectively paralyzed since January 2024, when AA fighters overwhelmed Myanmar military forces and captured the strategic town.

"Paletwa isn't just another border skirmish, It's the lynchpin of a project that provides our northeastern states with vital maritime access while reducing dependence on the vulnerable Siliguri Corridor."

The **Kaladan project,** under development since 2008, aims to create a transportation network linking Kolkata to Sittwe port in Myanmar, then up the Kaladan River to Paletwa, before connecting to Mizoram via road. Prior to the AA offensive, the project had shown significant progress, with cargo operations between Kolkata and Sittwe launching in May 2023.

The AA takeover came as part of "Operation 1027," a coordinated campaign by various resistance groups systematically capturing strategic locations from Myanmar's military junta since October 2023. The conflict has devastated Chin State, one of Myanmar's poorest regions, where ethnic Chin communities have long suffered from marginalization and military abuses.

Complicating matters for Indian policymakers is the AA's apparent selective targeting. Security analysts note that while Indian infrastructure projects face disruption, Chinese investments remain largely untouched. This dynamic plays out against India's recent pledge to support railway connections to Chin State.
There's clear evidence suggesting coordination between the AA and Beijing. This fits China's regional strategy of establishing alternative trade corridors.

In recent weeks, AA leadership has suggested willingness to allow the project's continuation under renegotiated terms that would increase their authority and financial benefits. Meanwhile, India has intensified diplomatic efforts with Bangladesh and Thailand to develop a coordinated response to Myanmar's fragmented political landscape.

As the standoff enters its second year, the future of this critical infrastructure project—and India's strategic ambitions in Southeast Asia—hangs in the balance, with Chin State caught in the crossfire of competing regional powers.

Fazlur Rehman's Warning and the Rising Separatist Wave in Pakistan

What It Means for India

Maulana Fazlur Rehman, a senior Pakistani politician and leader of the Jamiat Ulema-e-Islam (JUI-F), recently issued a stark warning about the potential disintegration of Pakistan. He cautioned that if certain districts of Balochistan declared independence, the United Nations might recognize their sovereignty, leading to a significant fragmentation of the country. His statement reflects the deepening crisis in Pakistan, where long-standing insurgencies, political instability, and economic decline are fueling separatist sentiments. Balochistan, in particular, has witnessed a decades-long struggle for autonomy, with multiple nationalist and separatist groups challenging Islamabad's authority. The situation has worsened as Pakistan's military response has been met with allegations of human rights violations, disappearances, and extrajudicial killings.

The unrest in Balochistan is not an isolated event but part of a broader pattern of instability that also includes Khyber Pakhtunkhwa, where Tehrik-i-Taliban Pakistan (TTP) has intensified its insurgency. The return of the Afghan Taliban to power in 2021 has emboldened militant groups operating in Pakistan, leading to a surge in attacks against security forces and government installations.

The growing influence of separatist groups, combined with the government's failure to address ethnic and economic grievances, has created a scenario where parts of Pakistan could spiral out of control. Maulana Fazlur Rehman's warning

comes amid increasing international attention on Balochistan, with reports of enforced disappearances and targeted killings drawing concern from global human rights organizations. If the province moves towards self-determination, it could trigger a chain reaction, further destabilizing Pakistan and reshaping South Asia's geopolitical landscape.

On March 11, 2025, militants from the Baloch Liberation Army (BLA) seized control of the Jaffar Express in Pakistan's Balochistan province, taking approximately 214 passengers hostage, including individuals suspected to be military personnel. The attackers halted the train by damaging the railway tracks, leading to an intense firefight with security forces that resulted in casualties. The BLA issued an ultimatum, demanding the release of Baloch political prisoners within 48 hours, warning that failure to comply would result in the execution of hostages and the destruction of the train. The rugged terrain and inadequate communication infrastructure have made rescue operations extremely challenging, further underscoring the growing instability in Balochistan.

The Tehrik-i-Taliban Pakistan (TTP) has reportedly formed a strategic alliance with the BLA, amplifying the effectiveness of insurgent operations in the region. This collaboration has facilitated coordinated assaults on Pakistani military outposts and security installations, significantly escalating the government's struggle to maintain control. The TTP's backing has provided the BLA with crucial logistical support, funding, and advanced combat tactics, thereby intensifying the unrest in Balochistan and complicating counterinsurgency efforts.

For India, Pakistan's internal strife presents both opportunities and risks. On one hand, a weakened Pakistan, struggling with internal conflicts, may have fewer resources to support cross-border terrorism or interfere in Kashmir. Indian security agencies have closely monitored the rise of insurgent movements in Balochistan, recognizing the strategic implications of a divided Pakistan. However, instability in Pakistan could also pose challenges, including an increase in refugee flows, a surge in radicalized militants spilling over into India, and the potential for nuclear assets falling into the wrong hands. The growing influence of China in the region, particularly its investments in Balochistan under the China-Pakistan Economic Corridor (CPEC), adds another layer of complexity. Beijing's concerns over attacks on its infrastructure projects could push China to exert greater influence over Pakistan's internal affairs, potentially reshaping power dynamics in South Asia.

Recent events further validate Fazlur Rehman's warning. The Baloch Liberation Army (BLA) and other separatist groups have carried out high-profile attacks, including a deadly assault on Pakistani security forces in Gwadar. In Khyber Pakhtunkhwa, TTP militants have openly clashed with Pakistani forces, challenging state authority. Additionally, Pakistan's worsening economic crisis, marked by soaring inflation and political infighting, has further eroded the government's control over restive regions. If the situation continues to deteriorate, Pakistan could face a scenario similar to the 1971 Bangladesh Liberation War, where a combination of internal rebellion and international pressure led to the creation of a new nation.

India must assess the evolving situation carefully. While the fragmentation of Pakistan could reduce threats along the western border, it could also lead to a more volatile and unpredictable security environment. Any instability in Pakistan could pus h extremist groups to seek safe havens elsewhere, including Afghanistan and even India's border regions. Additionally, India's strategic interests in the Indian Ocean and connectivity projects with Iran and Central Asia could be affected if Pakistan descends into chaos. New Delhi must maintain a balanced approach—monitoring developments closely while strengthening its security apparatus to prevent any spillover effects from Pakistan's internal crisis.

Maulana Fazlur Rehman's warning is not just a political statement but a reflection of a rapidly unfolding crisis. With separatist movements gaining momentum, Pakistan faces an uncertain future, one that could reshape the region in ways that will directly impact India. As Islamabad grapples with its growing instability, New Delhi must remain vigilant, ensuring that any developments across the border do not disrupt its own national security and strategic interests.

Youth Clubs in Kerala

A Closer Look at Radicalization Trends

The southern State of Kerala in India illustrates a case of unfortunate polarity. It, while being the most literate state, is also home to one of the deadliest radicalization drives that has been taking place in the country.

As far back as in 2017, the Kerala police have reported that approximately 100 individuals from Kerala have joined ISIS, however, it is likely that the actual number of recruits from the region is significantly higher. The issue of politically supported radicalization is contributing to the state's current challenges and could lead to its downfall.

Political and Religious Links:
Organizations like Jamaat-e-Islami Hind (JIH) Kerala, Indian Union Muslim League (IUML), and the now-banned Popular Front have been involved in fostering radical sentiments.

The Solidarity Youth Movement (SYM), JIH's youth wing, in 2023, has hosted controversial figures like former Hamas leader Khaled Mashal.

Protests by the Muslim Students Federation (IUML's student wing) have also raised concerns. The previous year, in 2022, the Muslim Students Federation of IUML staged protests against Catholic schools in the state that enforced a ban on the hijab within their premises.

It is, however, the wide network of political groups' affiliated sports & cultural clubs operating both within Kerala and abroad; and targeting children, teens, and youths alike, which pose a serious challenge to Indian agencies' efforts at de-radicalization and consequently counter-terrorism.

Various sports and cultural clubs act as platforms for promoting radical views. Growing Influence and Radicalization:

The use of **sports, arts, and cultural events** helps these groups engage youth and shape their ideologies.

Young individuals exposed to these radical narratives from a young age are at risk of further radicalization and recruitment into extremist activities.

Green Star Arts and Sports Club (GSASC) has branches across Kerala and even abroad (UAE). Its events have included pro-Palestinian demonstrations.

Lightning Arts & Sports Club (LASC), another similar organization, witnessed solidarity displays with Palestine at its **Koduvally** chapter.

Malarvadi Bala Sangam (MBS), an initiative under JIH Kerala, targets children up to 7th grade. Despite its focus on arts and cultural activities, it has been linked to subtly spreading radical ideology.

Security Concerns:
Youth clubs in Kerala have been used by local politico-religious groups to spread propaganda, exploiting younger generations' interest in sports and arts. This exposure can lead to distorted worldviews and recruitment by extremist terror outfits. Monitoring of activities of the local youth clubs is the grave need of the hour for Indian security agencies for the state of Kerala, which is already grappling with the threat posed by the Islamic State.

From 100 km away

A wake up call for India's National Security

The device was set up on the north shore of Qinghai Lake @CAS

China, the first-mover unveiled a new milestone in the laser-based spy camera system acclaimed as the world's most advanced, capable of capturing a person's facial scars or the serial number of satellites from 100 km away. Featuring synthetic aperture LIDAR, over 100 megapixel with 8K resolution and spotting precision of 1.7mm, this technology significantly revolutionizing the earth observation satellites, likely escalates serious concerns to India's national security amid simmering tensions with its northern neighbour.

This technology outmatch the capabilities of everyday cameras such as mobile phones, DSLR or even the drones which are ubiquitous in defence and civilian life nowadays. If this could be deployed in lower earth orbit, zooming into individuals on the ground with chilling details or anything with an accuracy of 156mm can be done. Its power reportedly, 100 times greater than the current spy telescopes. Though many Chinese researchers claim it's a prototype, the implications are immediate and profound.

Challenges for the system
Still the system faces significant challenges, relies on stable weather conditions, less cloud cover and atmospheric conditions can affect image quality. It also struggles to capture moving objects due to the need for extreme precision.

What does this mean to India?
For India, the stakes are acute. A tussle between both countries in the Line of Actual Control, where the satellite images are often exposes China's atrocities or illegal advancement. Meanwhile this camera could enable the neighbour to surveillance Indian troop movements, missile sites, military or naval bases in real time. Apart from land territorial threat, it could also pose a significant threat to India's satellites. "This isn't just about seeing a satellite – it's about reading its serial numbers", a Beijing based imaging scientist reportedly highlighting China's edge in space espionage. The United States, once a leader with Lockheed Martin's 2 cm resolution at 16 km in 2011, has questioned its own tardiness and expressed alarm through its media. Yet, in India, public discourse remains muted, leaving a gap in awareness and urgency.

China's claimed objectives are broad and include extensive reconnaissance of competing satellite designs and facial recognition of "enemies" from orbit, including Taiwan, America, and terrorists. Given the underfunding of the Vibrant Villages Program along the LAC, this could jeopardise border security for India. If China uses this technology in small, covert units, drone warfare which is already changing Indian battalions with pilot instruction from gamers will reach new heights.

Strategic Implications
In the future, small drones equipped with these advanced imaging systems could become highly effective tools in both defense and offense.
The ability to remotely monitor enemy soldiers, gather intelligence on enemy positions, and even conduct strikes with pinpoint accuracy could make drones an indispensable part of military operations.

India's increasing use of drones for defense purposes, such as monitoring its borders, underscores the urgency of keeping pace with these advancements. As drones grow more integral to contemporary warfare, the ability to observe and interpret ground activities from hundreds of kilometers away could fundamentally reshape the battlefield.

India must act
The emergence of such powerful surveillance systems raise concerns about critical national security. India must consider how these innovations could affect the defence and security strategies. There is an urgent need to focus on competitive inventions to ensure that India competes with the global power.

Online training of terror recruits

A dark side of the Digital Age

In March of this year, Indian security agencies have arrested one Abdul Rehman, who allegedly planned to target the Ram Temple in Ayodhya. He reportedly confessed to being linked to the Islamic State Khorasan Province (ISKP). The most striking aspect of this case, however, is that he received all of his training online, via video calls, while attending full-time to his shop in Milkipur

While terrorist outfits are adapting well to the digital age and using it to carry out propaganda and radicalization is common knowledge, online training of terror recruits presents another challenging phenomenon which is surprisingly not even new.

A case in point is that of Mohammad Zaki Amawi's, a U.S. citizen. After failing to enter Iraq for combat in March 2004, Amawi returned to Ohio and began gathering jihadist training materials online to form a local group in Toledo. He compiled resources, including a "Basic Training" course and instructional videos on IEDs and suicide bomb vests. The group also practiced at a shooting range in Toledo, while Amawi communicated with jihadists in Iraq for technical guidance.

Another case is that of a Dell laptop captured in Syria in 2014, which belonged to an ISIS recruit. Buried in the "hidden files" section of the computer were 146 gigabytes of material, containing training manuals for executing Islamic State operations -including videos of Osama bin Laden, bomb construction guides, vehicle theft directives, and materials on using disguises to evade capture.

As late as in 2022, the report by Tech Against Terrorism found at least 198 websites run by global terrorist and extremist groups on the surface web. Analyzing 33 notable sites, including those of Islamic State, al-Qaeda and the Taliban, revealed they attract around 1.54 million monthly visitors.

Terrorist organizations, through their websites and dedicated online channels, provide digital manuals and videos on weapon use and planning attacks. Virtual training through simulations helps recruits with tactics and logistics. Some groups recruit "lone wolves" online for small attacks.

Additionally, they teach cyberterrorism techniques and encourage use of dark web and encrypted applications to communicate and disseminate instruction materials among potential recruits. In 2015, the Islamic State (IS) even ranked chat applications by encryption levels: SilentCircle, Redphone, and Signal were 'Safest'; Telegram, Wickr, Threema, and Surespot were 'Safe'; and WeChat, WhatsApp, Hike, Viber, and Imo.im were 'Unsafe'.

Closer home, Pakistan's Jamaat-ud-Dawah (JuD), a front for the banned Lashkar-e-Taiba, reportedly used gaming apps to indoctrinate youth into jihad against India, as noted by Indian Intelligence agencies in 2020. As an outcome to many such findings, the Indian government in 2023 banned 14 mobile applications reportedly used by terrorists in Jammu and Kashmir, including Wickrme, Mediafire, Briar, BChat, Nandbox, Conion, IMO, Element, Second Line, Zangi, Threema, Crypviser, Enigma, and Safeswiss.

Easy access, anonymity, and global reach make the internet attractive to terrorist groups to reach out to and radicalize individuals, promoting the exchange of information and the planning of violent acts, both physical and cyber. Although there are initiatives in place to track online activities and eliminate extremist content, the sheer volume of material and the possibility of anonymity pose significant challenges in preventing radicalization and recruiting new members.

Institute of Objective Studies (IOS)

Just another academic body, or there's more than meets the eye?

INSTITUTE OF OBJECTIVE STUDIES

In October of 2024, the Enforcement Directorate seized properties of the Kozhikode office of the Institute of Objective Studies (IOS) as part of its investigations into the now-banned Muslim organization **Popular Front of India (PFI).**

IOS is a prominent academic body with a main office in New Delhi and chapters across several major cities in India. A close study of the institutional and organizational linkages of IOS in general however sparks additional concerns about its agendas.

The PFI connection
Prof. P. Koya, a key member of PFI was the coordinator for the Kozhikode chapter of IOS and was involved in IOS activities. In 2017, IOS co-organized an international conference on 'The role of women in making a humane society' alongside the National Women's Front (NWF), the women's wing of PFI. **Dr. M. Manzoor Alam**, Director of IOS registered his presence at the event as well.

Indian institutional and individual associations
IOS' strong ties with political strongmen are visible from the fact that Sam Pitroda, Chairman of the Indian Overseas Congress and a figure close to the Gandhi family has delivered lectures at IOS on several occasions. Congress veterans namely Salman Khursheed, Saleem Ahmed, Meem Afzal, and Late Ahmed Patel have also shared ties with IOS in the past. Its director Dr. Alam was spotted interacting with West Bengal Chief Minister (CM) Mamta Banerjee as early as in 2011.

In 2021, IOS facilitated the Late Maulana Syed Jalaluddin Umri, the former Ameer of **Jamaat-e-Islami Hind (JIH)** with an achievement award. Prof. M. Afzal Wani, the current Chairman of IOS has also spoken at multiple JIH-sponsored events.

In the same year, IOS alongside the Falcon Group of Institutions co-organized a Muslim Leadership Conference which was attended by prominent leaders, religious heads, and businessmen from the Muslim community of India.

Links with educational institutions
IOS is part of a well-connected network of educational institutions and universities, both in India and internationally. Within India, IOS tie-ups are with the likes of **Jamia Milia Islamia, Aligarh Muslim University, Darul Huda Islamic University, and Maulana Azad University.**

On the International level, Turkish universities and the Organization of Islamic Countries (OIC)- sponsored International Islamic University, Malaysia (IIUM) are among IOS' frequent collaborators.

Ties with foreign governments
The IOS has close ties with the Turkish government and its sponsored bodies. This is exemplified by the fact that a delegation of IOS openly expressed their solidarity with the Turkish government in the face of a failed coup attempt in 2016. Besides, Prof. Selim Argun, vice president of religious affairs of the Republic of Turkey was personally present at an IOS event in 2019. It is pertinent to note that even PFI is known to have a shared association with the **Turkish government** and its sponsored bodies.

In 2019 itself, IOS' director Dr. Alam met Prince Turki Alfaisal of Saudi Arabia and discussed means of finding and enhancing cooperation between organizations and centers of research.

Foreign NGOs & IOS
It is however the direct and indirect linkages of IOS with controversial foreign NGOs which warrants a threat.

In 2023, Safaa Zarzour- the President of the **USA-based Islamic Society of North America (ISNA)** spoke at a virtual conference organized by the IOS. ISNA is the charity front of the Muslim Brotherhood (MB) in the US and has been alleged to have financed extremist groups, including the **HAMAS** in the past.

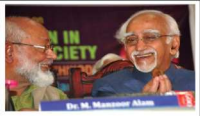
International Institute of Islamic Thought (IIIT), a US-based non-profit is another frequent collaborator with IOS. Its founder-president Hisham Altalib is famously a Muslim Brotherhood sympathizer. IIIT was investigated by US federal authorities in the aftermath of the 9/11 attacks for funding Al-Qaeda and other terrorist groups.

In February of 2018, Dr. Aroub AYAH Alrifai, Member, of General Assembly, **Int'l Islamic Charitable Organization (IIICO), Kuwait** addressed an IOS event. IIICO is another MB-affiliated body that has been sanctioned by Israel for alleged ties to HAMAS.

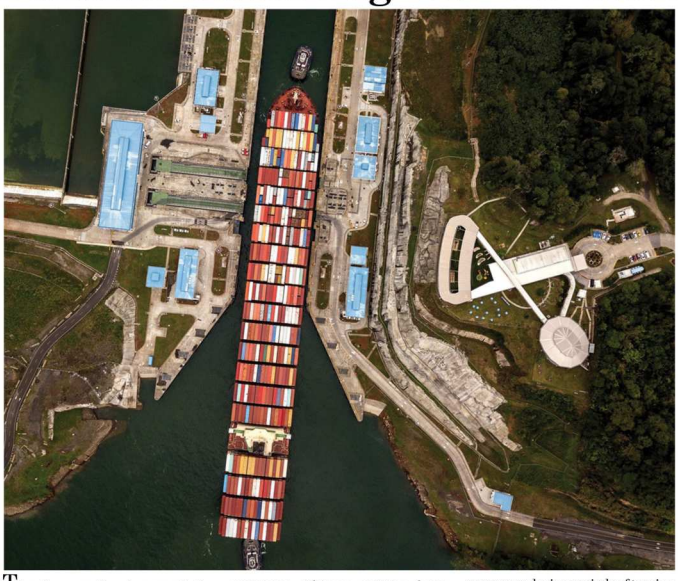
Controversial views and ideas
Writings of IOS' key members and its published reading materials do give slight insights into the anti-government and staunchly pro-Muslim agenda guiding its functioning. Dr. Manzoor Alam, through his articles and in his interviews has consistently portrayed Muslims in India as the oppressed minority faction and the government as discriminatory towards them. His 2003 article titled 'Reflections On Contemporary Indian Situation' stands as testimony to his views. As a body, IOS also has time and again organized events on such themes as the need to protect mosques, reclaim Waqf properties, and strict adherence to the principles of Islam.

The Institute of Objective Studies has been in existence since 1986 and has, over the years, come up to forge critical alliances with national and international partners, not all of which are without controversies and thus raising concerns about its agendas, in the context of India's internal peace and security.

Row over Hamid Ansari attending PFI conference



Panama Canal Tug-Off US-China Relations



The Panama Canal, one of the world's most critical maritime passages, has emerged as the latest flashpoint in escalating tensions between the United States and China, following controversial claims made by US President Donald Trump.

In his recent inaugural address, President Trump alleged that Panama has surrendered control of the canal to China and claimed Chinese troops are stationed there—assertions firmly denied by both Panamanian authorities and Beijing officials.

While Panama retains operational control of the 82-kilometer artificial waterway, Chinese entities have established a significant economic presence in the surrounding infrastructure. Hong Kong-based CK Hutchison Holdings has operated two critical terminals—Balboa on the Pacific side and Cristóbal on the Atlantic side—for over two decades. Additionally, China became the second-largest user of the canal after Panama joined the Belt and Road Initiative in 2017, with Chinese shipping now representing approximately 21% of goods passing through.

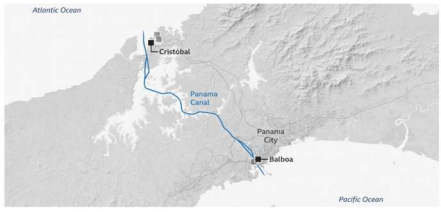
US security experts have expressed concerns that Chinese-operated ports could monitor US naval movements and potentially disrupt commerce during periods of tension. Some analysts worry these civilian facilities might conceal covert Chinese military or intelligence assets under commercial cover.

In what appears to be a response to these growing concerns, CK Hutchison has reportedly agreed to sell its port operations to US-based investment firm BlackRock—a move widely interpreted as an American effort to counter Chinese influence. Panamanian authorities have also recently announced an audit of CK Hutchison's port operations.

Despite China's growing footprint, the United States remains the canal's largest user, with approximately 3.5 times more goods passing through to the US than to China. Panama's experience with the Belt and Road Initiative has reportedly fallen short of expectations, with several promised Chinese projects either shelved or failing to materialize.

As climate change continues to threaten the canal's operations—evidenced by recent drought-induced restrictions—and geopolitical tensions rise, the strategic value of this waterway is likely to increase further. Panama now balances precariously between competing superpowers: one that built its famous canal and another investing billions in its future development.

The waterway that once symbolized American engineering prowess now reflects a changing world order, as Panama navigates the delicate diplomacy of maintaining relationships with both Washington and Beijing.



Syria's Landscape

This fractured landscape represents the new reality of a once-unified state transformed into a geopolitical laboratory where regional ambitions and global rivalries continue to unfold at tremendous human cost.

Since 2011, Syria has been transformed into a complex proxy war where major powers have fought for influence and strategic advantage. Russia's interest in the Syrian war is shaped by a mix of strategic, military, and geopolitical factors. First, Syria is a long-standing ally, and by supporting Bashar al-Assad, Russia seeks to maintain and expand its influence in the Middle East, countering Western, especially U.S., dominance in the region. The presence of vital Russian military bases in Syria, including a naval facility in Tartus and an airbase in Hmeimim, provides Russia with a strategic foothold in the Mediterranean, allowing for greater power projection.

The United States maintains a small but strategic presence in Syria's oil-rich eastern provinces—with troops guarding facilities that produce an estimated 80,000 barrels per day, according to energy sector reports.

Iran views Syria as the crucial western link in its "Axis of Resistance," providing a land corridor to Hezbollah in Lebanon. Intelligence sources indicate Iran has invested over $30 billion in military infrastructure and proxy militias throughout the conflict.

This new agreement could significantly alter the geopolitical landscape. For Russia, it strengthens its ally Assad's control and potentially diminishes American influence. For Turkey, Kurdish reconciliation with Damascus might address its border security concerns without further military action. Iran gains from any consolidation of its ally's power, while the United States faces challenging questions about its continued military presence.

Behind these strategic calculations lies a humanitarian catastrophe of staggering proportions. The UN continues to document atrocities, with entire families being killed amid ongoing violence despite reduced international media attention.

As regional powers recalibrate their positions, Syria's tragedy continues to demonstrate how geopolitical interests often override humanitarian concerns in modern conflicts, with ordinary Syrians paying the highest price for these global power games.

China's Expanding Presence in Geostationary Orbit

China's growing presence in the geostationary orbit (GEO) is raising security concerns due to unpredictable satellite movements, which have significant defense implications, experts warn. As China continues to expand its satellite fleet, it is positioning itself as a dominant force in space, driven by both commercial and military interests.

At the Chatham House Space Security 2025 conference in London on March 5, experts discussed the increasingly erratic behavior of Chinese spacecraft in GEO. This orbit, located 35,786 kilometers above the equator, is crucial for communications, intelligence, and military operations, making it a key strategic area for space dominance.

China has been rapidly expanding its satellite fleet in GEO with communications, remote sensing, and classified spacecraft. These satellites, often described as experimental communication satellites, are believed to have advanced capabilities, including proximity maneuvers, satellite inspections, missile early warning, and electronic signals intelligence. These capabilities allow China to alter its satellites' positions in GEO, enabling them to conduct targeted operations, such as intercepting communications or monitoring foreign satellites.

These GEO satellites are sliding or moving very frequently, which is uncharacteristic of satellites intended for communication such behaviors are seen as a potential military threat, raising alarms about China's growing ability to maneuver and potentially disrupt or damage foreign satellites.

A recent example is the launch of the TJS-15 satellite on March 9, part of a series of experimental Chinese spacecraft conducting proximity maneuvers in GEO. These maneuvers could allow China to inspect foreign satellites and even intercept communications. Juliana Suess from the German Institute for International and Security Affairs (SWP) warned that while China's activities are not entirely undetectable, its ability to conduct precise maneuvers and hide actions in real time is becoming a growing concern.

China's space activities align with its broader defense strategy to militarize space. The Chinese Communist Party (CCP) has made it clear that space is critical to its national security, and it is investing heavily in developing technologies to dominate the space domain. China's military is particularly focused on capabilities to disrupt or neutralize adversary satellites, which would give it a significant strategic advantage in future conflicts.

One example of China's increasing space-based defense capabilities is the Shijian-25 satellite, launched in January. This satellite is capable of refueling and servicing other spacecraft on orbit, extending their operational life. The Shijian-25 follows the Shijian-21, which successfully docked with a defunct Beidou satellite and moved it to a higher orbit. These capabilities suggest that China is not only focusing on satellite deployment but also on extending the functionality of its space assets, which could be used to support military operations. As of now, China has approximately 1,000 satellites in orbit, a dramatic increase from just 40 in 2010. This rapid growth in space assets is seen as part of China's broader strategy to enhance its space-based defense and intelligence capabilities, posing a growing challenge to the U.S. and its allies.

"We see great risk right now because of the unprecedented growth, as well as the unmanaged competition in space," said Lerch, reflecting concerns over the increasing militarization of space. With its expanding presence in GEO, China is solidifying its position as a major player in the space domain, with potential consequences for global security and defense.

Thailand Deports Uyghurs to China Amid International Outcry

In a controversial decision, Thailand deported 40 Uyghur men back to China in February 2025, drawing sharp criticism from human rights groups and global governments. The men had been detained in Thailand for over a decade after fleeing China to escape persecution. Despite offers from several countries, including the U.S., to resettle the refugees, Thailand chose to send them back to China, where they face potential torture and forced labor.

Thai officials defended the move, citing security concerns and the country's diplomatic ties with China. The government argued that the deportations complied with international legal norms, but critics contend that Thailand prioritized its relationship with China over the safety of vulnerable individuals. Human rights organizations fear that the Uyghurs will face severe consequences upon their return to China, where they are already subject to widespread abuse in the Xinjiang region.

The United States and other Western nations had urged Thailand to reconsider, offering alternative resettlement options. However, Thailand stood firm, stating it had little choice but to comply with Beijing's demands, fearing economic and diplomatic repercussions.

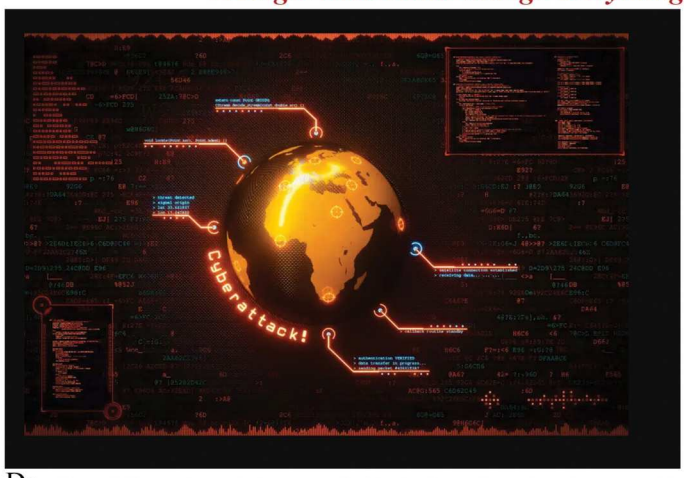
Analysis

The deportation highlights the complex dynamics between human rights and geopolitics. For Thailand, maintaining strong ties with China is vital for trade and investment, particularly under China's Belt and Road Initiative. As nations like Thailand balance economic interests with human rights, the case demonstrates the challenges of standing up against powerful authoritarian regimes.

The incident has sparked renewed calls for stronger international action to protect refugees, especially those from oppressed groups like the Uyghurs. It also underscores the growing tension between global human rights standards and pragmatic political decisions.

Between Satellites and Cyber Warfare Iran's Digital Offense

A single click could change everything



Dr. Elena Rodriguez knew something was wrong the moment the email landed in her inbox. Written in impeccable English with a seemingly innocent subject line about professional opportunities, the message carried a dangerous payload that could compromise an entire satellite network.

Satellites and Cyber Swords

Since launching three satellites in recent months, Iran has demonstrated growing technological capabilities that extend far beyond simple communication. Their Noor satellite series, first launched in 2020, represents a significant leap in the country's aerospace technology, blurring lines between civilian and military satellite programs.

In the tense months following the October 7 Israel-Hamas conflict, Iranian cyber threat actors have become increasingly sophisticated. Groups like APT42 and UNC1549 are no longer just hacking—they're conducting precision digital operations that could potentially cripple critical aerospace infrastructure.

The Language of Deception

The attack vectors are meticulously crafted. An email might include subtle linguistic triggers:

- Words like "جنگ" (war in Farsi)
- Phrases like "משאומתן" (negotiations in Hebrew)
- Seemingly innocuous job application language

Dr. Gregory Falco, an MIT-trained aerospace security expert, explains the real danger: "It's not about breaking down doors anymore. It's about finding the smallest crack in the system and quietly sliding through."

Networks Under Siege

Potential targets are strategically critical:

- U.S. and Israeli government satellite networks
- Commercial aerospace communication systems
- Hospital communication infrastructures
- Nuclear activity monitoring systems

Real-world statistics underscore the threat:

- Iranian cyber attacks increased by 50% in the last year
- Aerospace systems experience an average of 22 significant cyber intrusion attempts monthly
- A single compromised privileged user account can provide access to networks tracking sensitive geopolitical information

The Human Weak Link

What makes these attacks so dangerous is their focus on human psychology. Threat actors understand that behind every secure system is a person – someone who might be tired, distracted, or simply curious about an unexpected email.

"These aren't random attacks," says a cybersecurity analyst who asked to remain anonymous. "They're carefully researched, precisely targeted, and psychologically engineered."

Invisible Frontlines

As Iran continues to advance its satellite capabilities – with recent launches demonstrating payload delivery to altitudes of over 500 kilometers – the digital landscape becomes increasingly complex. Traditional warfare has expanded into a realm where a computer screen can be as dangerous as a battlefield.

For professionals like Dr. Rodriguez, vigilance isn't just a professional requirement—it's a critical line of defense in an invisible, ongoing conflict.

India Acts Against Russian Crypto Exchange

GARANTEX

Indian officials helped uncover the exchange in a coordinated international blitzkrieg to take down Garantex, a Russian crypto exchange accused of ties to money laundering. This massive crackdown, spearheaded by the U.S. Department of Justice (DOJ) and supported by countries including Germany and Finland, led to the seizure of Garantex's infrastructure and freezing over $26 million in proceeds of crime.

In a statement released on March 12, 2025, India's Central Bureau of Investigation (CBI) announced the arrest of Garantex co-founder Besciokov from the South Indian city of Thiruvananthapuram, as he was planning to flee the country.

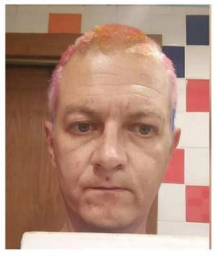
He was said to have been apprehended while vacationing with his family in Varkala.

India's Central Bureau of Investigation (CBI), alongside the Kerala Police, apprehended Aleksej Besciokov, a Lithuanian national who acted as a principal administrator of the exchange, in Kerala. Besciokov is charged with money laundering, sanctions violations and facilitating transactions tied to ransomware. Now he will have to confront extradition proceedings for the United States.

Garantex was said to have processed $96 billion in cryptocurrency transactions since its launch in 2019, including over $6 billion in

transactions conducted after the U.S. Treasury sanctioned it in 2022. The exchange had evolved into a multi-faceted haven for criminal behaviour such as ransomware payoffs and darknet market transactions.

This operation is a testament to what competent and informed coordination can achieve and further establishes India's standing as a proactive and proactive partner in tackling international cyber and cryptocurrency-related crime. But experts warn that the platforms are prone to rebranding to sidestep restrictions, and thus remain a persistent headache for regulators globally.



Lithuanian national
Aleksej Besciokov

Bio-Weaponization of Blood

What are they making?

While the military's intentions may be noble—saving the lives of soldiers on the battlefield—the technology itself raises troubling possibilities for misuse. Military advancements are often cloaked in secrecy, and what starts as a tool for humanitarian aid could easily spiral into the development of biological weapons. What if the technology that enables synthetic blood also opens the door to blood-based bioweapons? In the future, could a nation create a weapon that targets the blood systems of its enemies, causing mass casualties without leaving a trace of traditional weapons?

This is not as far-fetched as it may seem. With modern genetic engineering capabilities, it may soon be possible to develop viruses or bacteria that specifically attack the blood, destabilizing entire populations. If this technology fell into the wrong hands, it could lead to catastrophic consequences. Blood engineering, under the guise of military necessity, could quickly turn into a tool for mass destruction.

Contamination Risks: A Silent Threat

Even if we set aside the prospect of weaponization, the logistics of blood engineering in combat zones present a significant risk. Blood storage and transfusions in the field are already fraught with dangers—imagine the complications when synthetic blood, which may not have the same properties as real blood, is introduced. Without proper storage or preparation, synthetic blood could cause adverse reactions, blood clots, or even immune system failures in soldiers who receive it.

In the chaos of a battlefield, where sanitation is a distant luxury, the risk of contamination could be multiplied. A single mistake in the handling of synthetic blood could infect entire battalions. Imagine a battlefield infection spreading like wildfire among soldiers, with the "miracle" blood now a silent killer rather than a savior.

The global community is aware of the potential dangers of blood engineering, and the technology could conflict with international laws governing biological weapons. The use of blood-based bio-weapons would likely violate the Biological Weapons Convention, and such advancements could push nations toward developing new forms of bio-warfare that are difficult to regulate or detect.

A More Sinister Agenda?

There's a growing suspicion that the push for advanced blood engineering in the military isn't just about saving lives—it may be part of a far more sinister agenda. What if the true goal is not simply to improve battlefield medicine, but to create something far more terrifying—a generation of enhanced, bio-engineered soldiers who are no longer fully human? With the ability to manipulate blood, genetic traits, and physical capabilities, could military powers be laying the groundwork for a new form of warfare, one that turns human beings into controllable, super-powered weapons?

The push for synthetic blood and genetic modifications could be a precursor to creating soldiers with abilities far beyond what is naturally possible—soldiers who may lack autonomy or even humanity itself. As this technology progresses, one can't help but wonder: Are we building a future where we no longer fight with conventional weapons, but with monsters of our own making? The possibility of such a nightmare is not as far-fetched as it might seem, and it raises an unsettling question: What is the real plan behind these developments?

Internet of Underwater Things (IoUT) as Next Step in Naval Domain

Madrid, Spain — Indra, a leading Spanish multinational in defense and technology, has been involved in several high-profile projects across the globe, including in China. Over the years, the company collaborated with Chinese defense and technology firms, particularly in satellite communication, cybersecurity, and radar systems. These partnerships raised concerns among Western allies, who feared the potential for sensitive military technologies to be shared with China. Indra's involvement in projects like China's Beidou satellite system and various defense contracts led to scrutiny, with some nations closely monitoring its relationships due to security risks associated with foreign influence on defense technologies. This history adds complexity to Indra's current innovations, such as the proposed "Internet of Underwater Things" , a new technology that could revolutionize naval warfare. This concept aims to build an interconnected network of sensors, robots, and unmanned vehicles to enhance surveillance, communication, and combat strategies in the ocean.

The IoUT would enable **real-time data sharing between underwater devices,** providing naval forces with improved situational awareness and faster responses to threats. Using a combination of sensors, autonomous underwater vehicles (UUVs), and artificial intelligence (AI), the system would offer continuous monitoring and instant communication between units in challenging underwater environments.

Indra's Chief Technology Officer, Carmen Fernández, explained that the IoUT would enhance precision and security **in underwater operations, making the oceans "smarter" and providing military forces with unprecedented capabilities. The system could transform naval tactics, improving the detection of threats, coordination of units, and reducing risks to human lives by deploying autonomous systems in dangerous environments.**

While the company is a major player in global defense technology, Indra has also faced scrutiny for its past dealings with China. In previous years, Indra worked with Chinese defense and technology firms, particularly in areas of satellite technology and cybersecurity, sparking concerns among international allies about its role in sensitive defense technologies. This history has led some countries to closely monitor the company's relationships, especially as it develops new technologies like the IoUT.

The IoUT proposal signals a major shift in naval strategy, offering nations a technological edge in underwater warfare. As defense contractors explore this concept, it could become a cornerstone of next-generation military technologies, despite potential geopolitical concerns surrounding Indra's past engagements.