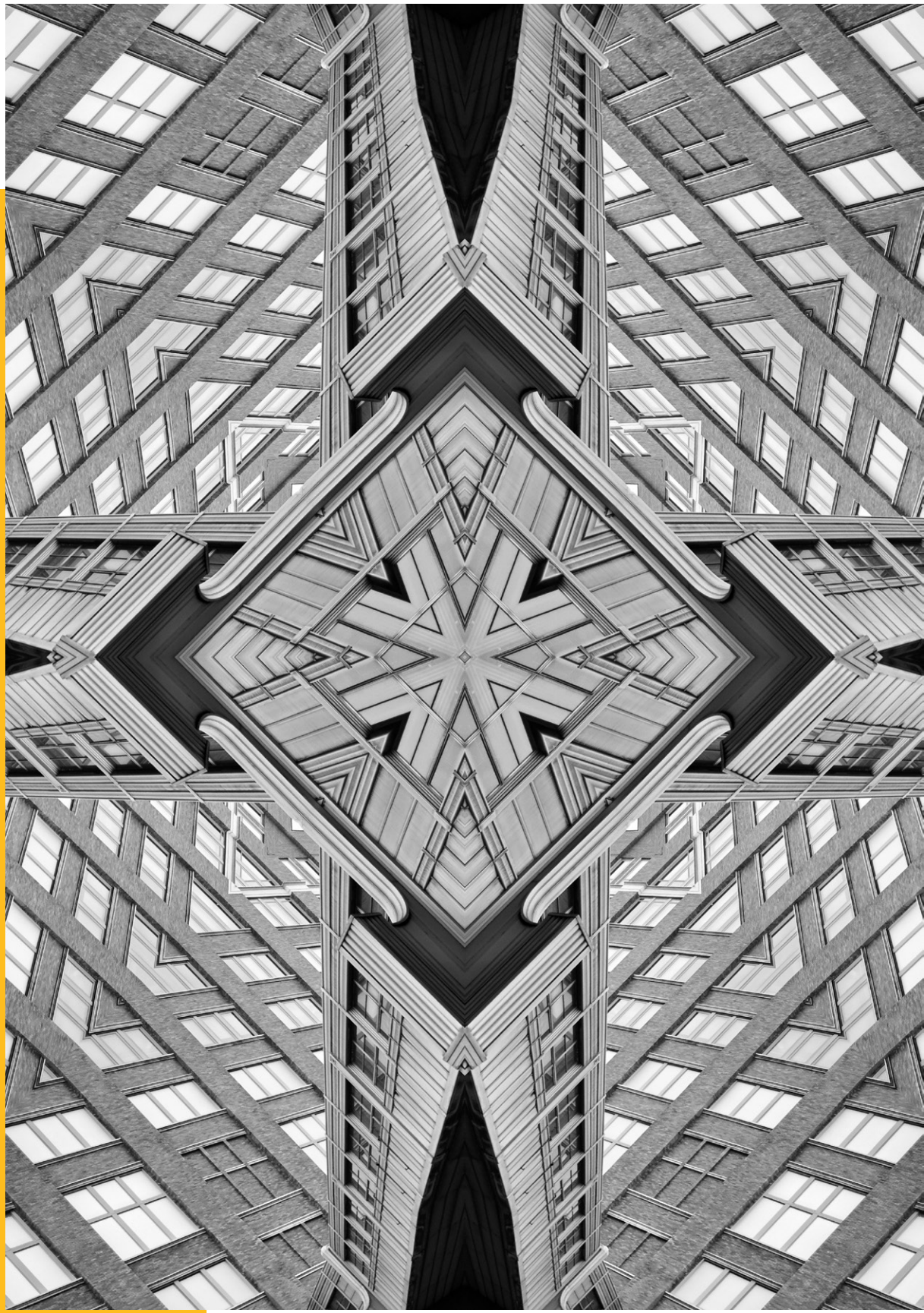
OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 514 JANUARY 2026

Swords and Shields: Navigating the Modern Intelligence Landscape

Samir Saran and Archishman Ray Goswami

Abstract

As key custodians of a nation's strategic intent, national intelligence services must account for and adapt to the wider socio-cultural and political factors shaping their operational environment. Today, shifting geopolitical tides in the form of accelerated multipolarity, scientific progress, and the erosion of accountability in global technological governance have converged to reshape national intelligence strategies. This paper seeks to make sense of these changes by discussing key features of the shifting global intelligence landscape. These include factors such as the role of 'geotechnography' in blurring distinctions between offline and online experiences, the consequences of growing inter-state competition over rare-earth elements and supply chains, the evolving character of human intelligence (HUMINT) amid ubiquitous technical surveillance (UTS), and the role of private sector intelligence and Big Tech in a data-infused geostrategic terrain. The aim is to foster a discussion on how nations think about and use intelligence in changing times. It closes with an exploration of the implications of these changes for India's national security.

Attribution: Samir Saran and Archishman Ray Goswami, "Swords and Shields: Navigating the Modern Intelligence Landscape," *ORF Occasional Paper No. 514*, Observer Research Foundation, January 2026.

Introduction

In his 1998 book, *Seeing Like a State*, social scientist James Scott articulated the concept of the *metis:* the naturally imbibed knowledge of social circumstances that actors can only gather from practical experience of said circumstances.[1] For Scott, this concept took the clearest expression in what he perceived as the state's innate panache for foreign policy and its associated "metis-laden" disciplines of war and diplomacy—this provides the cognitive basis upon which policymakers may adapt to rapid geopolitical, strategic, and tactical change while "making the best out of limited resources."[2]

Scott's premise holds a unique value for national intelligence services reckoning with the incendiary geopolitics of the 2020s. Rapid advancements in communications technology have enabled today's wars to break past the constraints of the local or regional with unprecedented pace to acquire a more global flavour. Today, it is easier than ever for a Mexican or Colombian drug cartel to send members overseas to acquire mastery over new strategies of drone warfare and ISR (or Intelligence, Surveillance, and Reconnaissance) honed on Ukraine's frontlines,[3] or for private military companies such as the United States (US)-based Academi to step in to provide strategic services to the embattled government of Haiti, struggling against gang violence.[a,4] Geopolitical volatility manifests in other ways too. Quick access to cheap, miniaturised, and technologically advanced military and commercial platforms has enabled non-state and proxy actors to deploy outsized strategic authority against conventionally stronger global powers to achieve their vested interests. And with the ubiquitous and pervasive forces of social media and instant communication reshaping the knowledge that guides how one interacts with and responds to their surroundings—in other words, one's individual *metis*—new and increasingly regenerative forms of transnational ideological affiliation and radicalisation are mushrooming.

It is this volatile techno-geopolitical landscape that contextualises and reshapes the character of national intelligence today. While geography structures strategic planning in national politics, the international politics of the 2020s is being defined by the redistribution of global power and the upending of entrenched hegemons. The change is both vertical and horizontal. It is embodied by the fragmentation of the integrated global economy of the 1990s by its very architects in the Global North, the reconfiguration of multilateralism as those Global North preeminent powers come to contend with an increasingly

a Academi was founded as Blackwater in 1997, and was used to provide security for US forces in Iraq in the early 2000s during the War on Terror.

Introduction

vociferous Global South, and the exponential pace of technological advancement that has elevated the profile of transnational digital giants to unprecedented levels, and centred scientific achievement as the primary metric of power and legitimacy within the international system.

Such geopolitical volatility has also brought to the fore key questions that national intelligence services, including India's own, must grapple with. How are new forms of social and political affiliation, gestated by the proliferation of digitally interconnected geographies, reshaping intelligence priorities? Are private intelligence actors challenging government intelligence agencies on their own turf, and if so, how can the latter adapt to this new reality? How is human intelligence (HUMINT) adapting to the ascendancy of open-source intelligence (OSINT) and ubiquitous technical surveillance (UTS)—the latter defined as "the widespread collection of data and application of analytic methodologies for the purpose of connecting people to things, events, or locations"?[5] How, in turn, can intelligence agencies secure national interest with the greatest efficiency by synthesising cross-informational flows across multiple sources, including public digital and commercial ones? And in an increasingly fractious world, how can India best integrate the core principles of its grand strategy into its approach to foreign intelligence?

These are some of the questions that this paper seeks to examine. To that end, it explores four key technological and geopolitical trends, and their implications for contemporary intelligence practice: digitally-connected transnational geographies; the global race for rare-earth elements (REEs); the changing nature of HUMINT amid the rise of UTS; and the role national intelligence can play in securing a nation's technological and supply needs, and the rise of private sector intelligence actors (PSIAs) within national security intelligence ecosystems. The paper concludes with an assessment of what India can do in light of these changes, emphasising on its potential as a bridging power through a measured expansion of existing liaison agreements with security partners.

Digital Geography and Changing Strategic Demands

Now in its fourth decade of existence, the public internet has entered a stage of its life where its broader social impact can be conclusively gauged over the long term. Digital communications today have made for a world that is as spatially small as it is socially fractured. The telescoped domain of cyberspace has, in many ways, bridged the constraints of physical geography, and contributed towards a world where new, trans-border forms of social and political affiliation may emerge more quickly. It challenges established ideological and cognitive frameworks, even as it expands the scope and speed of narrative construction and dissemination worldwide by both state and non-state actors. This rise of "geotechnography"—"a collision of geography, technology, and society" typified by the "despatialisation" engendered by contemporary digital technologies and the friction between natural human "rootedness in land" and the conflicting "new sense of self built by engaging with social media and other global digital platforms"—presents unprecedented challenges and opportunities for national intelligence services, and is reflected in the emergence of new strategies developed within this context.[6]

As social media collapses distances between continents, ideology has become increasingly prone to intersectionality. Whereas the spread of transnational forms of social or political association was once restricted by the limitations of physical geography and analogue technology, immediate digital communication across social media platforms has made it easier for such forms of identity to spread faster and at scale. In the days after the 7 October attacks by Hamas on Israel, and Israel's ensuing response, the war in Gaza emerged as a flashpoint around which groups of otherwise different stripes—from left-wing activists to proscribed Islamist organisations—rapidly coalesced, aided by the scale and ubiquity of social media.[7]

Indeed, the scale of Gaza-related movements since 2023 speaks to the wider role that geotechnography has come to occupy within the contemporary global security landscape. Amplified by social media, the dynamics of an otherwise regional conflict have rapidly entered the daily lexicon of domestic politics and forged unlikely partnerships between activists of varied political stripes. Intelligence services monitoring these trends must therefore prepare for the rapid spread of political movements shaped by transnational affiliation and their wider implications for national security.

Unlike in the past, where revolutionary political ideologies such as Marxism reached a certain stage of theoretical maturation and stability before being gradually disseminated by the forces of early-20th century society and technology, geotechnography today makes for the rise of ideologically amorphous and more volatile forms of social and political identity for intelligence services to

contend with in order to maintain internal security. The rise of such "salad-bar extremism"— where a discerning diner can pick and choose aspects from a global smorgasbord of political and extremist beliefs to fit their stance at any given time—portends a more capricious security landscape for governments into the near future.[8]

Added pressures on decision cycles—as a result of geotechnography and the rapid construction of narrative and frameworks of social/political affiliation by way of social media and other digital mechanisms—have contributed towards the rise of strategic intelligence disclosure (SID) and the renewed focus on strategic communications as a dimension of contemporary intelligence activity.[9] Faced with the prospect of facing weaponised narratives that rapidly connect and self-perpetuate across disparate geographies through digital media, national intelligence services—long accustomed to maintaining total secrecy over the information they hold—have been compelled to strategically declassify parts of the intelligence they hold in order to construct counter-narratives of their own.

In the lead-up to the war in Ukraine in February 2022, Western intelligence services, fearing the prospect of a Russian assault on Ukraine where the Kremlin held the informational advantage, embarked on a process of strategic declassification, aimed at pre-empting Russian strategic communications in the event of Ukraine's invasion.[10] The purpose of this operation had been the establishment of a public-facing credible premise for the Western counter-response that seemed increasingly inevitable. As narratives become increasingly easy to construct and broadcast through digital media for purposes of subversion, SID is likely to grow as a form of anticipatory, and even coercive, variant of intelligence activity.

Finally, the puncturing of physical geography by digital tools and the transnational connections it gestates necessitates a closer focus on global challenges even by medium-sized intelligence bureaucracies traditionally focused on developments within their region. Key global intelligence services, such as Israel's Mossad[11] and India's Research and Analysis Wing (R&AW),[12] have historically been focused on security developments within their own neighbourhood, gathering intelligence and prosecuting covert action with a regional focus. At a time when physically distant forms of identity have been brought into closer dialogue by the forces of geotechnography, it is incumbent upon national intelligence agencies—including those with a traditionally regional focus due to both budgetary and strategic constraints—to develop the analytical capabilities to better relate global developments to local ones in order to pre-empt the proliferation of sudden, volatile forms of social and political identity in a more fractious geopolitical landscape.

Despite the increased power of digital media to erode some geographical limitations, physical geography continues to bear vital influence on geopolitics today. Perhaps nowhere is this clearer than with regard to the geopolitics of rare-earth elements (REEs)—an increasingly central feature of the modern security landscape. Just as competition over energy and other mineral resources drove conflict over the past century and in recent decades, from uranium and coltan in the Congo to oil in the Middle East, the estimated growth of global industrial demand for REEs by between three to sevenfold by 2040 will likely shape the international politics in the coming years.[13] This has already been demonstrated by the US-Ukraine Minerals Deal of April 2025,[14] and closer to home, Pakistan's efforts to attract US investment and strategic backing in the form of a critical minerals agreement.[15] The securitisation of commerce in the REEs space suggests new roles for national intelligence agencies to adopt in helping their governments to establish strategic advantage in this domain.

As with the wider question of geotechnography, establishing an intelligence advantage for oneself within the global REEs environment will require governments to dedicate more resources to enable their intelligence services to have a global mission and reach. Global supply chains, including REEs, tend to be distributed across a variety of interconnected national jurisdictions. Emblematic of the kind of "weaponised interdependence" that international relations scholars such as Henry Farrell and Abraham Newman describe, such global dispersal enables adversaries to apply pressure at any single point to leverage against one's own state.[16] Securing the state against such threats will require national intelligence services, including those that are more regionally-focused, to develop the required assets and capabilities to deploy globally, and thus maintain one's strategic edge in a more competitive age.

Covert action—primarily through acts of sabotage and denial—are similarly likely to be used by national intelligence services to prevent adversaries and competitors from acquiring or developing a strategic advantage in the global REEs landscape, just as it was often deployed during the Cold War as superpowers rushed to secure raw materials for their fissile programmes and national deterrents, most notably during the Congo Crisis of the 1960s.[17] Recent intelligence operations such as the Mossad's so-called 'Operation Grim Beeper' in September 2024 targeting pagers and handheld radios owned by Hezbollah fighters and cadres in Lebanon, have demonstrated the ability of the world's most powerful intelligence services to embed themselves within supply chains to deliver kinetic effect against adversaries.[18]

Translated into the world of REEs, these principles can be re-applied to the denial or disruption of competitors' rare-earth supply chains. In Myanmar, rebels of the Kachin Independence Army (KIA) have taken advantage of the country's ongoing civil war to cement their control over key rare-earth deposits of dysprosium and terbium, leveraging its control over the deposits to grow its relationship with neighbouring China as an (illicit) trade partner to the north.[19] Its actions may serve as a sign of things to come—one where intelligence-linked special operations forces (SOF)/insurgent outfits are leveraged by competing nation-states to deny opponents access to REEs supply chains in order to maintain one's own advantage.

Mining REEs is also accompanied by environmental concerns that may be leveraged against competitors by national intelligence services. As local activism increasingly becomes a target for politicisation and espionage by national intelligence services, the possibility of obstructing adversaries' REE ambitions through a variety of kinetic efforts, including astroturfed activism and information warfare, is a real one. Indeed, national intelligence services such as the UK's Secret Intelligence Service (SIS) have already declared "green spying"—the use of measurement and signature intelligence (MASINT), imagery intelligence (IMINT), and other means to gather intelligence on the total carbon emissions produced by states—as a top priority.[20] The danger of such 'green spying' and its weaponisation in coordination with other tools, such as the SID described above, is considerable, and may be leveraged to pre-emptively limit competitors from achieving strategic advantage and autonomy within the global REEs landscape.

Despite the rise of digital tools of espionage, the human aspect of intelligence—the standard fare of the global espionage landscape, involving human spies in target nations gathering secrets and facilitating operations—will endure. However, it will need to adapt to a new, increasingly transparent age. While the temptation in such an age may be to turn away from HUMINT in favour of OSINT, a more effective strategy—one articulated by a variety of intelligence scholars—would preserve the human component at the heart of espionage, while informing its use with an appreciation of the ascendancy of OSINT and digital tools. Yet although its strategic importance remains undiminished, HUMINT in the 2020s is clearly heading into a new era, one where OSINT can be utilised by private actors to uncover state secrets and deception, and the rise of UTS poses unprecedented difficulties to the standard requirements of maintaining cover or conducting espionage activities in hostile states.[21]

Social media and the permanence of one's digital footprint have made it increasingly difficult for intelligence officers to maintain cover and avoid detection by the governments they are spying against. This dimension of modern espionage has birthed its own branch of intelligence activity, called social media intelligence (SOCMINT), defined as "the surveillance and analysis of open platform social media social media sources", and is dovetailing with the rise of the OSINT industry.[22]

The emergence of such digitally-driven forms of 'generated reality' and espionage forces a rethinking of how intelligence is conceived, beyond the simple collection of secret intelligence or the processing of vast amounts of data gathered through both secret and commercial or public channels. It has similarly come to underpin intelligence competition between great powers such as the US and China, and been recognised as such by the two, with the Federal Bureau of Investigation (FBI) broadcasting warnings and advertorial films to warn service members of the risks.[23] The emergence of SOCMINT and OSINT as independent branches of intelligence has also been driven by organisations such as Bellingcat, which have utilised a combination of social media metadata and other digital tools across commercial and digital platforms to uncover the identities of foreign intelligence officers. Bellingcat's exposure of Olga Kolobova in 2022, a Russian GRU operative based in Europe under the alias 'Maria Adela', captured not only the changing character of this landscape but also the growing power of commercial tech actors within this space.[24]

Beyond the digital realm, traditional HUMINT operations must contend with the rise of what observers often refer to as UTS. As governments increasingly invest in surveillance technologies to further UTS for reasons of public safety or control, it has become more difficult for human spies to operate undetected despite the use of sophisticated tradecraft. Intelligence professionals increasingly note the difficulty of operating undetected in heavily digitally-surveilled cities, with even adversary counterintelligence services relying on UTS rather than physical surveillance of enemy agents and intelligence officers to track and impede simple acts of tradecraft, from organising meetings between case officers and their agents to concealing their identity or presence even within highly populated urban agglomerations.[25] Advances in biometric technology can be used to stop the entry of spies at a nation's border or limit the availability of foreign passports to be used by other agencies in their own operations.[26]

Yet while the rapid pace of technological advancement may make for a more transparent world where the standard cloak-and-dagger fare of traditional espionage would become obsolete, HUMINT will not only endure but grow increasingly valuable—as hinted at in a December 2025 speech by the chief of Britain's SIS, Blaise Metreweli.[27] In a more fractured geopolitical landscape, governments will require access to both high-grade intelligence at the level of an adversary's political and elite leadership to maintain decision advantage, and also at the lowest rungs of its strategic apparatus, and even within its civil society. Indeed, the digitally-fuelled transparency challenging the basic tenets of the intelligence profession is likely to drive a return to the analogue tradecraft of HUMINT. As former Central Intelligence Agency (CIA) officer and intelligence scholar David Gioe has noted, "Technological sources provide vast volumes of intelligence, but HUMINT remains fundamental for truly understanding adversaries' capabilities and intentions."[28]

Israel's intelligence failure on 7 October 2023, for instance—caused partially by its initial neglect of HUMINT reports in favour of digital surveillance tools against Hamas—shows that even in a digitally-underpinned strategic landscape, maintaining decision advantage and security necessitates a strong focus on HUMINT.[29] Additionally, as states seek to deliver kinetic effect against adversaries through covert action, a reliance on human operative is likely to persist.

Such HUMINT operations, however, will need to be conducted alongside cyber-operations and a sophisticated hold over technological innovation in the fields of AI and biometrics. As formal intelligence officers come under greater scrutiny by adversary counterintelligence services utilising UTS to their advantage, intelligence services have increasingly returned to the use of agents operating under 'non-official cover' (NOC), i.e., where intelligence officers operate informally and without the protection of their governments or the cover of diplomatic immunity.[30] Russia's Soviet-era Illegals programme—where intelligence officers are sent to target countries to assimilate and operate for years and even decades under deep cover as citizens of that country—continues unabated, particularly in countries such as Argentina and Slovakia, where identities are easier to obtain and local counterintelligence systems are weaker.[31]

Given the enduring importance of HUMINT even at a time when geolocation, metadata mining, and open-source tools have made it easier for private investigators to uncover state secrets, national intelligence agencies are also likely to dedicate more time and resources to technologies able to circumvent today's advanced biometrics and facial recognition systems. While exact details regarding such innovation remain highly classified, recent developments provide hints of the importance this issue has been accorded in recent years within contemporary intelligence thinking. The appointment of Metreweli as Chief of the SIS in October 2025 reflects some of these trends.[32] Metreweli, whose previous position was Director-General of the agency's 'Q' Division, tasked with managing technology for in-house use, is alleged to have led projects meant to secure the identities and covers of British intelligence officers or predict and evade increasingly sophisticated biometric surveillance technologies.[33] Her experience and subsequent appointment as chief of Britain's foreign intelligence service underscores a wider trend within the global intelligence landscape, one where technological innovation to mitigate against the challenges of UTS to HUMINT is prioritised, holding the potential to determine the primary objectives of a national intelligence service, and the possible career incentives of delving into such a space for its officers.

Private Sector Intelligence: Partner or Competitor?

Intelligence is no longer the monopoly of the state. Rapid technological advancement and the growing salience of whole-of-system approaches to national security have contributed to the rise of private sector players as intelligence actors, with tectonic ramifications for national intelligence services. These relationships have been well-documented. Edward Snowden's disclosures in 2013 about the US government's siphoning of user data from tech firms like Google, Yahoo, and other social media companies—often without their knowledge—caused a brief rift between the US national security company and Silicon Valley.[34] The rift is rapidly healing though, with the US intelligence community now among the largest buyers of commercially available data (CAI) available from Big Tech companies.[35] Likewise, governments have a long and storied history of cooperation with private sector intelligence actors (PSIAs), with the private detective agency Pinkerton, for instance, having worked with both business elites in 19th-century United States against trade unions, and the Union government against the Confederacy during the American Civil War (1861-1865).[36]

To be sure, the balance of this dynamic has shifted in recent years. Public-private partnerships have grown in scale, particularly in the technological domain, which intersects more closely than ever with geopolitics. Yet even as such partnerships have significantly augmented the strategic standing of engaged governments, through the production of cutting-edge innovations, they are equally threatened by adversaries seeking to acquire or otherwise undercut the technological advantage possessed by such states as a result of engagement with the private sector. In such circumstances, PSIAs have become increasingly central to the global intelligence landscape, especially given their expertise in such domains as corporate espionage and geopolitical risk—harbingers of a new generation of corporate security that overlaps almost routinely with international geopolitics. Of these, the former, once viewed as primarily the prerogative of business conglomerates, is now increasingly utilised by revisionist powers such as China to purloin technological expertise.

China's actions are mainly targeted against the United States, and its technological muscle that is primarily sequestered in the startup ecosystem of Silicon Valley, itself increasingly the target of corporate and industrial espionage conducted by PSIAs acting as proxies or fronts for rival powers.[37] It also conducts industrial espionage, against smaller countries such as the Netherlands and its robust semiconductor manufacturing ecosystem,[38] besides its purported ally Russia, where industrial secrets about critical defence technologies have allegedly been stolen by China's intelligence services through

private contractors.[39] Unlike the strategic bureaucracies of foreign countries—long the focus of national intelligence services—the private sector possesses its own cultures, organisational structures, and repositories of strategically sensitive material. With their expertise in collecting such information for mainly corporate entities, PSIAs are equally, if not better placed than their government counterparts in navigating the distinctive topography of the private sector.

As with corporate espionage, conducted through both cyber and analogue human means, geopolitical risk is another domain where PSIAs have established a first-mover advantage over national intelligence agencies. Intelligence gathered by PSIAs is often processed into risk analysis reports for business clients, summarising the overall challenges and opportunities of investing or beginning operations in a certain place or region arising from its geopolitics.[40] Such information guides subsequent decision-making within global businesses and conglomerates, and is even quantified within the insurance premiums placed on later activities, generating precedents that determine the extent to which a country can attract foreign investment.[41] Through such processes, PSIAs, and the geopolitical risk companies they often work alongside, hold the ability to alter real-world geopolitics and geoeconomics. National intelligence services, traditionally focused on state-sponsored threats, or at most, counterterrorism, must therefore increasingly adapt to a world where PSIAs have secured first-mover advantage by providing bespoke solutions to private sector businesses—a role that the government has traditionally been separated from in free-market economies.

At another level, the accumulation of vast quantities of user data by large tech firms and social media megacorporations, and the subsequent rise of what social scientist Shoshana Zuboff has described as "surveillance capitalism"—the commodification of personal data by large digital conglomerates "to manipulate and control the emotions of populations"—has further augmented the power held by private sector actors within the global intelligence landscape.[42] Once a monopoly enjoyed by those states possessing advanced technologies to collect data from digital platforms in pursuit of national security, governments and their spy agencies now increasingly rely on "commercially available information", sourced and often purchased from private corporations, as evidenced by a January 2022 report to the former Director of National Intelligence Avril Haines in the United States, published under the erstwhile Biden administration and outlining the US intelligence community's strategy for gathering and purchasing big data from private sector actors.[43]

Today, private data providers such as Amazon Web Services conduct the primary cloud computing services for the UK's three primary intelligence services—SIS, MI5, and GCHQ[44]—as well as for those of the United States—the CIA, FBI, and the NSA through its "Secret Region" programme.[45] Examples such as these point towards the growing power of private-sector/Big Tech actors as stakeholders within contemporary intelligence, besides raising questions surrounding the traditionally sacrosanct position of national sovereignty in international politics and citizen rights.

Yet they equally provoke questions for a nation's sovereignty and security: PSIAs, transnational corporations, and social media giants, like their counterparts elsewhere in the state sector, are not only driven primarily by commercial interests, but operate with far less oversight than the latter. While this has advantages for an attacking party that aims to leverage cooperation with such firms for access to vast quantities of an adversary's data, it leaves it equally vulnerable to reliance on such an entity which, in pursuit of commercial interests, may do the same for said adversary.

Recent incidents in India have once again brought the double-edged nature of such cooperation to the fore. During Operation Sindoor in May 2025, Pakistani terrorist organisations were reported to have collected imagery, intelligence, and data on Indian military movements from commercial satellite imagery platform Maxar technologies—which was, in parallel, being used by India's armed forces.[46] Likewise, prayers made in Delhi High Court in November 2025 have pointed to the possible mass harvesting of passenger data by consultancy firm KPMG from the DigiYatra smartphone application.[47] Examples such as these demonstrate some of the associated risks of working with private sector firms with limited accountability, particularly in the intelligence and national security space.

Going forward, national intelligence services must adapt to an increasingly fraught intelligence landscape, where they are no longer the primary stakeholders. As corporate espionage bleeds into national security, and assessments of geopolitical risk within the private sector increasingly determine the geoeconomic trajectories, government spies will need to adapt their skills, while involving themselves more deeply within the world of PSIAs using a combination of offensive, defensive, and passive means. The growing power of Big Tech, propelled by their access to enormous quantities of data beyond the reach of even large intelligence services, portends massive changes within the global intelligence landscape.

Implications for India

India's emergence as the world's fourth largest economy in the world, and according to the Lowy Institute Asia Power Index, the third most powerful state in the continent, demands a recalibration of its intelligence strategy.[48] Such a reordering must be underpinned by recognition of the changes within the global intelligence landscape discussed in this paper, and an ability to adapt to them on the basis of internal course correction and external diplomacy.

The complexity of global supply chains and its weaponisation by adversaries has implications for India's national security, creating a greater role for the intelligence services within this space. Ensuring supply chain security is particularly important with regards to REEs, a matter that acquires greater urgency given the near monopoly of China in this sector and the export restrictions strategy that it is implementing. This can potentially trigger a scramble for securing alternative sources. In this context, the civil war in Myanmar assumes significance as geopolitical competition over its mineral resources has been a key driver of conflict. Since 2021, Chinese intelligence services have actively supported and sponsored proxy insurgent groups and ethnic armed organisations (EAOs) in mineral-rich regions of the country, squeezing India's supply chains and leaving New Delhi vulnerable to pressure from Beijing.[49] Calibrated violence has also been exercised by both the Burmese junta and insurgent groups in the vicinity of India's regional connectivity projects, enabling adversaries to set a precedent of leveraging control over vital supply chain nodes for short-term gains.[50] As India grows, and likely contends with a broader variety of competing state and non-state actors in regions like Myanmar endowed with (rare-earth) mineral reserves, it must take steps to establish the necessary countermeasures to both plug vulnerabilities against exploitation, and escalate the costs of such aggression for potential competitors.

Similarly, the growing centrality of geopolitical risk within international trade presents a range of challenges and opportunities for India's national security for which the country's intelligence services must be prepared. Geopolitical risk assessments play an increasingly important role in factoring into insurance premiums and business decisions, particularly amid the splintering of the post-1991 global economic order.[51] Fluctuations within global insurance rates has outsized impact on global trade, and may even be weaponised by proxy agencies and organisations acting on behalf of competing states. As geopolitics acquires greater importance within the C-suite, and economic security increasingly underpins national security, national intelligence services, including India's, will need to pay greater attention to its implications for India's economy and international trade, and particularly the role of PSIAs as primary actors of interest within this area. In this context, Indian intelligence agencies will need to equip themselves by developing a niche understanding of key trends in geoeconomic intelligence.

Implications for India

They will also need to adapt tradecraft and strategies as HUMINT evolves, and nations compete for technological superiority for quicker and streamlined processes of all-source assessment and intelligence analysis. Recent media reports suggest that Indian intelligence have been primarily reliant on TECHINT in dealing with internal security challenges, often at the expense of HUMINT.[52] While the foreign intelligence picture is less clear, such reports point toward key gaps within India's intelligence architecture. A greater emphasis on growing its HUMINT capacities while remaining cognisant of the technological constraints shaping it, is vital.

Reforms within India's intelligence apparatus in the past decade have established the foundations for future adaptation. The Multi-Agency Centre, the primary intelligence-sharing network for India's intelligence services, was upgraded in early 2025, with a greater focus on real-time intelligence analysis and streamlining.[53] The setting up of the National Intelligence Grid has complemented this information sharing between agencies by linking their databases. The intelligence successes in Operation Sindoor in May 2025 suggest closer cooperation between India's foreign and domestic intelligence agencies, a far cry from the bureaucratic infighting that has long characterised inter-agency relations.[54] Moreover, efforts have been made to grow intelligence diplomacy with all stakeholders in mineral-rich, strategically sensitive spaces within India's neighbourhood, such as in Myanmar.[55] All of these point towards growing political will to tailor intelligence requirements to a changing geostrategic landscape. It also underlines that, to a certain extent, Indian intelligence agencies will need to shed their reticence to undertake more diplomatic engagements to advance national interests.

At the diplomatic level, India's primary strength within the global intelligence landscape lies in its potential as a bridging power, leveraging its ability as a liaison partner to exercise greater influence on the world stage, while remaining cognisant of the counterintelligence concerns that inevitably accompany any decision to share intelligence with partner states. The minilateralism characterising much of India's foreign policy today equally defines the nature of the intelligence liaison platforms that it leads or participates in.

The Indian Navy's Information Fusion Centre-Indian Ocean Region (IFC-IOR), based in Gurugram, for example, enables New Delhi to share maritime signals intelligence with a number of regional and global partners, and augments India's position within the region as a liaison partner.[56] Likewise, the Colombo Security Conclave—convened by the National Security Advisors of India, Sri Lanka, the Maldives, Mauritius, and Bangladesh—provides a useful

mechanism for the sharing of intelligence within manageable frameworks, despite challenges posed by domestic instability within other member states such as Bangladesh.[57] India's strategic autonomy also burnishes its credentials as a bridging power within the global intelligence landscape, convening intelligence chiefs from around the world, often representing nations in conflict or competition, in New Delhi once a year.[58]

India's bilateral intelligence-sharing partnerships will also support its efforts to adapt to the strategic realities described previously. Technological liaison through frameworks such as the initiative on Critical and Emerging Technologies (iCET) signed with the erstwhile Biden administration in the US, followed by the implementation of the TRUST framework in 2025 with President Donald Trump, has enabled India to equip its intelligence services with the resources to adapt to a changing global security environment.[59] Yet India must also remain aware of the imbalanced power dynamic baked into such an equation, given today's great-power transactionalism and propensities for leverage.

India may equally choose to develop formal strategies around the use of SID for purposes of effective strategic communication. In a more transparent world, governments have increasingly taken to strategic declassification of portions of their intelligence (after properly sanitising it) as a means of coercive public diplomacy against adversaries, seeking to delegitimise and galvanise international pressure against them. Western agencies, for instance, continuously publicised SIGINT and imagery intelligence (IMINT) about Russian troop movements along Ukraine's borders in late 2021 and early 2022 to buy time ahead of what had come to be seen as an inevitable Russian military operation against Ukraine.[60] Russia too, has employed a similar strategy—having intercepted communications among Germany's military staff on the supply of Taurus missiles to Ukraine in early 2024, and released it on RT, Russia's state broadcaster.[61]

India itself is no stranger to its use, with the R&AW having intercepted, taped, and subsequently 'leaked' Pervez Musharraf's telephone calls to military commanders during the 1999 Kargil War to prove Pakistan's culpability as an aggressor.[62] Yet a more formalised doctrine (classified or otherwise), centred around audio/audio-visual intelligence/satellite imagery, and packaged for audiences accustomed to more visual means of news consumption on platforms such as social media, would buttress India's own strategic communications.

Implications for India

The national security implications of weaponised geopolitical risks also demand change within the mandate of India's national intelligence services. The domains of geopolitical risk, and the rise of PSIAs require new forms of expertise and engagement with the private sector in domains ranging from technology to international finance. The establishment of In-Q-Tel, a venture capital firm focused on emerging technologies, by the CIA in the late 1990s, has helped the US maintain its strategic and technological edge over both partners and competitors today.[63] This paper recommends that the government dedicate resources to a similar fund for the R&AW. Establishing smooth liaison channels with India's indigenous R&D ecosystem, much of which exists as part of the private sector, is vital, emphasising self-sufficiency as India grows as an independent power in a more competitive world.

Conclusion

The sheer pace of technological advancement, geopolitical volatility, and social change, combined, have produced unprecedented challenges for today's spy services. It raises new questions, some of which are as philosophically-infused as they are policy relevant. In a changing geopolitical and technological order, what really is the new final frontier for national intelligence services?

As the speed of processing, synthesising, and disseminating intelligence becomes as vital as the traditional mechanics of sensing and responding, what new mantles will intelligence communities worldwide be required to take on? In a digital environment increasingly permeated with deepfakes and sophisticated AI imagery and data, how can they discern truth from deception in order to secure national polities—while avoiding the propensity to perceived politicisation as agents of censorship? And do these shifts suggest that technology is blurring the lines between 'upstream' strategic and 'downstream' tactical information—just as 9/11 and the ascendance of counterterrorism as a national security priority broke down the walls between foreign and domestic intelligence in the first two decades of this century?

Adapting to these fast-paced changes demands strategic agility even as states grapple with these existential questions. Yet as the world heads into the mid-2020s, the geopolitical winners of tomorrow will be those whose intelligence services can most credibly demonstrate this kind of adaptability. The stakes are high, and none more so than for India, as it looks to the future with renewed confidence and optimism.

Samir Saran *is President, ORF.*

Archishman Ray Goswami *is Non-Resident Junior Fellow, ORF; and a DPhil International Relations candidate at the University of Oxford.*

Endnotes

1 James Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1998), pp. 6-7.

2 Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, pp. 315.

3 Henry Ziemer, "The Future of Criminal Drone Use in Latin America," *War on the Rocks*, September 9, 2025, https://warontherocks.com/2025/09/the-future-of-criminal-drone-use-in-latin-america/

4 "Blackwater Founder to Deploy Nearly 200 Personnel to Haiti as Gang Violence Soars," NPR, August 15, 2025, https://www.npr.org/2025/08/15/nx-s1-5503316/blackwater-erik-prince-haiti-gang-violence

5 Office of the Inspector General: Audit Division, *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*, Washington DC, Department of Justice, 2025, https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

6 Samir Saran and Anirban Sarma, *Geotechnography: Mapping Power and Identity in the Digital Age* (Gurugram: Penguin Random House India, 2025), pp. xiv-xv.

7 Tara Varma and Kevin Huggard, "France Responds to the Israel-Gaza Crisis," *Brookings*, December 15, 2023, https://www.brookings.edu/articles/france-responds-to-the-israel-gaza-crisis/

8 Alexander Meleagrou-Hitchens and Moustafa Ayad, *The Age of Incoherence? Understanding Mixed and Unclear Ideology Extremism*, Program on Extremism, Washington DC, George Washington University, 2023, https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/the-age-of-incoherence-final.pdf

9 DV Gioe and Michael Morrell, "Spy and Tell: The Promise and Peril of Disclosing Intelligence for Strategic Advantage," *Foreign Affairs* 103, no. 3 (2024): 138-152, https://www.foreignaffairs.com/united-states/spy-and-tell-gioe-morell.

10 Joakim Brattvol, "Intelligence Disclosure As A Strategic Messaging Tool," NATO, December 16, 2024, https://archives.nato.int/uploads/r/nato-archives-online/0/b/1/0b1691efa2718c16b63a16cc08c168381cf6a61fca31c04064991855a97e0279/2024-12-16_Intelligence_disclosure_as_a_strategic_messaging_tool_ENG.pdf

11 Tamir Libel, "Looking for Meaning: Lessons from Mossad's Failed Adaptation to the Post-Cold War Era, 1991–2013," *Journal of Intelligence History* 14, no. 2 (2015): 90, https://www.tandfonline.com/doi/abs/10.1080/16161262.2015.1033238.

12 Kajal Basu, "A 'RAW' and Present Danger," *The Indian Express*, December 7, 2023, https://www.newindianexpress.com/opinions/2023/Dec/06/a-rawand-present-danger-2639197.html

Endnotes

13 Mureji Fatunde, "The Race to Produce Rare Earth Elements," *MIT Technology Review*, January 5, 2024, https://www.technologyreview.com/2024/01/05/1084791/rare-earth-materials-clean-energy/

14 Gracelin Baskaran and Meredith Schwartz, "What to Know About the Signed U.S.-Ukraine Minerals Deal," CSIS, May 1, 2025, https://www.csis.org/analysis/what-know-about-signed-us-ukraine-minerals-deal

15 "US Strategic Minerals Signs MoU on Critical Minerals in Pakistan," US Embassy and Consulates in Pakistan, September 8, 2025, https://pk.usembassy.gov/u-s-strategic-metals-signs-mou-on-critical-minerals-in-pakistan/

16 Henry Farell and Abraham Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 43, https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic.

17 Jasmine Owens and Tara Drozdenko, "The DRC and America's Nuclear Weapons," Outrider Foundation, February 28, 2019, https://outrider.org/nuclear-weapons/articles/drc-and-americas-nuclear-weapons

18 John Paul Rathbone, Max Seddon and James Kynge, "How Israel's 'Operation Grim Beeper' Rattled Global Spy Chiefs," *Financial Times*, December 27, 2024, https://www.ft.com/content/f578b6c0-d534-4a04-ae25-3b97d11b6e71

19 Timothy McLaughlin, "A Rebel Army Is Building a Rare-Earth Empire on China's Border," *Bloomberg*, July 18, 2025, https://www.bloomberg.com/news/features/2025-07-18/as-us-and-china-feud-over-rare-earths-rebels-control-myanmar-s-mines

20 "MI6 'Green Spying' on Biggest Polluters to Ensure Nations Keep Climate Change Promises," *Sky News*, April 30, 2021, https://news.sky.com/story/mi6-green-spying-on-biggest-polluters-to-ensure-nations-keep-climate-change-promises-12286458

21 Shawn Benson, "Intelligence After Next: Deciphering Ubiquitous Technical Surveillance with Data-Driven Analytics and Artificial Intelligence," *MITRE Corporation*, June 11, 2024, https://www.mitre.org/news-insights/publication/deciphering-ubiquitous-technical-surveillance

22 Robert Dover, "SOCMINT: A Shifting Balance of Opportunity," *Intelligence and National Security* 35, no. 2 (2020): 227, https://www.tandfonline.com/doi/abs/10.1080/02684527.2019.1694132.

23 "The Nevernight Connection," FBI – Federal Bureau of Investigation, September 30, 2020, https://www.youtube.com/watch?v=N5V7G9IBomQ

24 Christo Grozev, "Socialite, Widow, Jeweller, Spy: How a GRU Agent Charmed Her Way Into NATO Circles in Italy," *Bellingcat*, August 25, 2022, https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/

Endnotes

25 "Ubiquitous Technical Surveillance Has Made Spying More Difficult," *The Economist*, July 1, 2024, https://www.economist.com/technology-quarterly/2024/07/01/ubiquitous-technical-surveillance-has-made-spying-more-difficult

26 "Revealed: the Advanced Technology Held in Our Passports," *Thales,* March 15, 2024, https://dis-blog.thalesgroup.com/identity-biometric-solutions/2024/02/22/revealed-the-advanced-technology-held-in-our-passports/

27 "Speech by Blaise Metreweli, Chief of SIS, 15 December 2025," *GOV.UK,* December 15, 2025, https://www.gov.uk/government/speeches/speech-by-blaise-metreweli-chief-of-sis-15-december-2025

28 David Gioe, "'The More Things Change': HUMINT in the Cyber Age," in *The Palgrave Handbook of Security, Risk, and Intelligence*, ed. Robert Dover, Huw Dylan, Michael S. Goodman (London: Palgrave Macmillan, 2017), 215

29 Michael Wyss, "The October 7 Attack: An Assessment of the Intelligence Failings," *CTC Sentinel* 17, no. 9 (2024): 4, https://ctc.westpoint.edu/wp-content/uploads/2024/10/CTC-SENTINEL-092024_cover-article-1.pdf

30 "Espionage Facts," International Spy Museum, https://www.spymuseum.org/education-programs/spy-resources/espionage-facts

31 Andrew Higgins, "How Two Russian Spies Went Deep Undercover with Their Children," *New York Times*, August 4, 2024, https://www.nytimes.com/2024/08/04/world/europe/russia-undercover-prisoner-swap.html

32 Chris Mason, Frank Gardner, and Rich Preston, "MI6 Appoints First Female Chief in 116-year History," *BBC,* June 16, 2025, https://www.bbc.com/news/articles/czxyx04dv1wo

33 Mason, Gardner, and Preston, "MI6 Appoints First Female Chief in 116-year History"

34 Shira Ovide, "The Spying That Changed Big Tech," *The New York Times,* September 16, 2021, https://www.nytimes.com/2021/09/16/technology/snowden-spying-big-tech.html

35 Andy Greenberg, Dell Cameron, Andrew Couts, "Security News This Week: The US Is Building a One-Stop Shop for Buying Your Data," *Wired*, May 24, 2025, https://www.wired.com/story/us-spies-one-stop-shop-private-data/

36 Rhodri Jeffreys-Jones, "Allan Pinkerton: Informed Scot or Scottish Reformer?," *Journal of Scottish Historical Studies* 42, no. 2 (2022): 198, 203-205.

37 James Titcomb, "Why Chinese Spies are Sending a Chill through Silicon Valley," *The Telegraph*, November 3, 2024, https://www.telegraph.co.uk/business/2024/11/03/chinese-spies-sillicon-valley-technology-google-apple-tesla/

Endnotes

38 Rory O'Neill, "Dutch Defence Minister Warns of Chinese Spying Threat," *Politico*, May 31, 2025, https://www.politico.eu/article/ruben-brekelmans-netherlands-china-spying-intelligence/

39 Jacob Judah, Paul Sonne, and Anton Troianovski, "Secret Russian Intelligence Document Shows Deep Suspicion of China," *New York Times*, June 7, 2025, https://www.nytimes.com/2025/06/07/world/europe/china-russia-spies-documents-putin-war.html

40 Katherine Tucker and Maria Robson-Morrow, "Intelligence Outsourcing for Non-traditional Clients: the Rise of Private Sector Intelligence Providers," *Intelligence and National Security* 40, no. 3 (2024): 413, https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2437958.

41 Prithvi Gupta, "Navigating Geopolitical Threats in the Insurance Sector," Observer Research Foundation, December 14, 2024, https://www.orfonline.org/expert-speak/navigating-geopolitical-threats-in-the-insurance-sector

42 Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York City: PublicAffairs, 2019)

43 Office of the Director of National Intelligence, *Senior Advisory Group Panel on Commercially Available Information*, Washington DC, Office of the Director of National Intelligence, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

44 Helen Warrel and Nic Fieldes, "Amazon Strikes Deal with UK Spy Agencies to Host Top-secret Material," *Financial Times*, October 26, 2021, https://www.ft.com/content/74782def-1046-4ea5-b796-0802cfb90260

45 Billy Mitchell, "Amazon to Launch Second Secret Cloud Region, Touting AI Innovation for National Security," *Fedscoop*, June 10, 2025, https://fedscoop.com/amazon-second-secret-cloud-region-ai-innovation-for-national-security-tulsi-gabbard/

46 "Weaponised Imagery: How Maxar's Satellite Data May Be Helping Pakistan And What India Can Do About It," Swarajya, May 9, 2025, https://swarajyamag.com/defence/weaponised-imagery-how-maxars-satellite-data-may-be-helping-pakistan-and-what-india-can-do-about-it

47 Pragya Singha Roy, "Data Evolve Accuses KPMG of Illegally Cloning Digi Yatra App in Delhi High Court," *TV 9*, November 28, 2025, https://www.tv9english.com/technology/data-evolve-accuses-kpmg-of-illegally-cloning-digi-yatra-app-in-delhi-high-court-article-10882779.html

48 Lowy Institute Asia Power Index: 2024 Edition, https://power.lowyinstitute.org/

Endnotes

49 Naw Betty Han, Shoon Naing, Devjyot Ghoshal, Eleanor Whalley and Napat Wesshasartar, "Exclusive: China-Backed Militia Secures Control of New Rare Earth Mines in Myanmar," *Reuters,* June 12, 2025, https://www.reuters.com/world/china/china-backed-militia-secures-control-new-rare-earth-mines-myanmar-2025-06-12/

50 "Kaladan Corridor: A Strategic Dream Marred by Ground Realities," *The Assam Tribune,* July 10, 2025, https://assamtribune.com/opinion/kaladan-corridor-a-strategic-dream-marred-by-ground-realities-1584235

51 Godwin O. Olasahinde-Williams and Mehmet Balcilar, "The Effect of Geopolitical Risks on Insurance Premiums," *Journal of Public Affairs* 22, no. 1 (2022): 1-12, https://onlinelibrary.wiley.com/doi/abs/10.1002/pa.2387.

52 Neeraj Chauhan, "India's Agencies Increasingly Depend on Tech Intel," *Hindustan Times,* January 9, 2021, https://www.hindustantimes.com/india-news/indias-agencies-increasingly-depend-on-tech-intel-101610160966455.html

53 "Amit Shah Inaugurates Revamped Multi-agency Network Built at ₹500 cr. to Fight Terrorism," *The Hindu,* May 17, 2025, https://www.thehindu.com/news/national/amit-shah-inaugurates-new-multi-agency-centre-connected-up-to-the-districts/article69584731.ece

54 Archishman Ray Goswami, "Cementing India's Intelligence Edge Against Pakistan After Operation Sindoor," Observer Research Foundation, May 27, 2025, https://www.orfonline.org/expert-speak/cementing-india-s-intelligence-edge-against-pakistan-after-operation-sindoor

55 "Indian Intelligence Chief Meets with Myanmar Vice Commander in Chief," *CNI Myanmar,* July 18, 2025, https://cnimyanmar.com/index.php/english-edition/30281-indian-intelligence-chief-meets-with-myanmar-vice-commander-in-chief

56 "Guardians Of The Indian Ocean: How India's IFC-IOR Is Transforming Maritime Security," *Dryad Global,* August 27, 2024, https://channel16.dryadglobal.com/guardians-of-the-indian-ocean-how-indias-ifc-ior-is-transforming-maritime-security-analysis

57 Sayantan Haldar, "The Colombo Security Conclave as a Much-needed Security Dimension," Observer Research Foundation, October 7, 2024, https://www.orfonline.org/research/the-colombo-security-conclave-as-a-much-needed-security-dimension

58 Dinakar Peri, "Amid Global Uncertainties, Spy Chiefs from Across World Converge in Delhi," *The Hindu,* March 16, 2025, https://www.thehindu.com/news/national/amid-global-uncertainties-global-spy-chiefs-converge-in-delhi/article69337785.ece

Endnotes

59 Prashant Jha, "TRUST Replaces iCET: New Brand, Old Spirit on Tech Partnership," *Hindustan Times*, February 14, 2025, https://www.hindustantimes.com/world-news/trust-replaces-icet-new-brand-old-spirit-on-tech-partnership-101739524899203.html

60 Kristian Gustafson, Dan Lomas, Steven Wagner, Neveen Shaaban Abdalla and Philip H. J. Davies, "Intelligence Warning in the Ukraine War, Autumn 2021 – Summer 2022," *Intelligence and National Security* 39, no. 3 (2024): 400-401, https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2322214.

61 Jessica Parker, "Singapore Sting: How Spies Listened in on German General," *BBC News*, March 8, 2024, https://www.bbc.co.uk/news/world-europe-68479836

62 Rajeev Deshpande, "Pervez Musharraf: An End with a Whimper and Not a Bang," *OPEN Magazine*, February 6, 2023, https://openthemagazine.com/feature/pervez-musharraf-end-whimper-not-bang

63 John Reinert, "In-Q-Tel: The Central Intelligence Agency as Venture Capitalist," *Northwestern Journal of International Law and Business* 33, no, 3 (2013): 677, https://scholarlycommons.law.northwestern.edu/njilb/vol33/iss3/4/.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org