RAMAIAH UNIVERSITY OF APPLIED SCIENCES

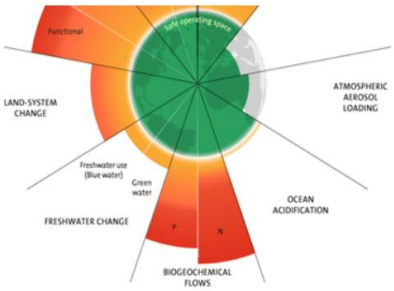
CENTRE FOR NATIONAL SECURITY STUDIES



VANTAGE POINT

A NEWSLETTER ON NON-TRADITIONAL SECURITY

FEBRUARY2026




Contents

Avian Influenza (H5N1): The Bird Flu That Refused to Stay in the Wings

Krithika Vijay

On a humid morning in May 1997, a three-year-old child in Hong Kong succumbed to a severe respiratory illness after exposure to infected poultry at a live-bird market. Laboratory analysis confirmed infection with the avian influenza A (H5N1) virus, marking the first documented instance of this avian virus crossing the species barrier to infect humans. This initial outbreak resulted in 18 confirmed human cases and six fatalities. It revealed, for the first time, that a virus long confined to waterfowl and poultry could pose a direct and lethal threat to humans.

Since that initial event, H5N1 has continued its unpredictable spread through domestic and wild bird populations and, more sporadically, through human hosts. As of early 2026, the World Health Organization (WHO) has reported approximately 970 to 990 confirmed human cases across about 25 countries, with 470 to 480 documented deaths. This translates to a case fatality ratio approaching 50 per cent, significantly higher than that of seasonal influenza. These numbers may *understate* the true burden, because mild cases may go undetected, and reporting systems vary widely by region. Still, they represent a sobering real-world tally - nearly a thousand people worldwide have been infected, and nearly half of them have died.

H5N1 is an Influenza A virus, an RNA virus with a segmented genome, a biological design that allows it to mix and match genetic segments when two viruses infect the same host at once. This 'genetic reshuffling' called reassortment is why influenza viruses evolve rapidly, and why scientists continually watch them for changes that could increase infectivity or host range. In birds, the virus is highly pathogenic, capable of killing flocks in a matter of days. Over the past decade, specific variants, particularly clade 2.3.4.4b, have circulated globally, resulting in widespread outbreaks of bird diseases across Asia, Africa, Europe, and the Americas. In some regions, the virus has even jumped into mammals, including marine animals and dairy cattle, raising additional concerns.

Human H5N1 infections remain rare and have not demonstrated sustained human-to-human transmission. Most cases result from direct contact with infected birds or contaminated environments. Clinical manifestations range from severe viral pneumonia to multi-organ failure, reflecting the consequences of a virus poorly adapted to human physiology. Public health agencies around the world monitor these cases carefully. A typical year may see a few dozen cases. In 2025, for instance, at least 26 human infections were reported globally between January and August, including deaths in countries like Cambodia, India, and Mexico.

Beyond its impact on people, H5N1 has been devastating for food security and economies. Poultry farming is the backbone of nutrition and income for millions globally. When an outbreak hits, mass culling is often the first line of defence. While effective for containment, it can devastate local food supplies, disrupt supply chains, and inflate prices. In many low- and middle-income regions, poultry is a primary protein source.

Losses whether due to disease or culling, can push vulnerable populations toward malnutrition and economic instability.

Epidemics such as H5N1 transcend public health domains, influencing trade, national economies, and governance. Poultry export bans, agricultural losses, and public anxiety fueled by misinformation can destabilize markets and erode trust in institutions. As global supply chains tighten and ecological pressures intensify, zoonotic outbreaks increasingly represent both a biological and geopolitical risk.

Science at the Forefront: What Must Be Done

For scientists and policymakers, the H5N1 story isn't just about chronicling outbreaks, but it is also about prevention and prediction. A few key scientific priorities are emerging:

- **Enhanced Genomic Surveillance:** Sequencing viral genomes from animal and human infections enables early detection of mutations that might increase human adaptability or transmissibility.
- **One Health Integration:** Human health, animal health, and ecosystem data must be connected, because a virus that moves through birds, mammals, and humans does not respect disciplinary boundaries.
- **Real-Time Data Sharing:** Transparent, rapid sharing of surveillance data across countries and institutions accelerates response times.
- **Preparedness Infrastructure:** From diagnostics to antiviral stockpiles, health systems need tools in place *before* a crisis hits.

The H5N1 story began in a bustling Hong Kong market nearly 30 years ago, but its chapters continue to unfold across continents, species, and scientific disciplines. The virus has not achieved sustained human transmission, a fact that tempers alarm, yet its persistence, evolution, and global footprint make it a pathogen worth watching.

This is a story of biology and human behaviour, of markets and microbes, of surveillance networks and scientific foresight. In that narrative, our actions - in labs, in farms, and in policy halls — will help determine what comes next. For, H5N1 has shown us that the threats that matter least to our awareness can matter most to our future.

Krithika Vijay *is a B.Sc. Biotechnology student at Ramaiah University of Applied Sciences, currently interning at the Emerging Technology vertical of CNSS. Her interests lie in biosecurity, cyber-biosecurity, and the science–policy interface, through which she brings a life sciences perspective to national security research.*

85 Seconds to Doomsday's Midnight: On the Urgency of Safeguarding Our Survival

Sruthi Kalyani

Human civilisation now stands at the closest margin to global annihilation in modern history. On 27 January 2026, the Bulletin of the Atomic Scientists advanced the Doomsday Clock to 85 seconds to midnight, down from 89 seconds in 2025. Established in 1947 at seven minutes to midnight, the Clock has long served as a barometer of existential risk, but the current setting marks the third time in five years that it has moved closer to catastrophe. The Bulletin explicitly attributes this acceleration to a systemic failure of leadership across global institutions and nation-states, signaling the onset of an era in which 'every second counts'. From a national security perspective, the ticking clock implies that the strategic environment is no longer governed by slow-moving and reactive structural changes but by mutually reinforcing emergencies that directly threaten our survival.

The decision to set the Clock at 85 seconds quantitatively reflects the disintegration of the post-Cold War security architecture. In 1991, the Clock reached its safest point at 17 minutes to midnight in 1991, following the end of the Cold War and the signing of the Strategic Arms Reduction Treaty (START I). Since then, this architecture has steadily eroded. The expiration of the New START Treaty threatens to remove the last remaining legally binding limits on intercontinental nuclear arsenals. This vacuum re-creates the structural conditions for a nuclear arms race for the first time in more than half a century. Proliferation concerns also arise in regional contexts such as Iran, India, and Pakistan, while aggressive posturing by Russia, China, and the United States further normalises nuclear signalling in conventional conflicts. Such re-nuclearisation of strategic competition compounds other systemic risks and stretches deterrence doctrines to breaking point.

The 2026 announcement not only warns about the dangerous resurgence of traditional nuclear threats but also about other seemingly slow yet drastically disruptive forces. In the climate domain, record heatwaves, droughts, floods, and the partial collapse of environmental monitoring systems indicate a failure to meet the Paris Agreement's temperature goals, aggravated by the rollback of clean energy incentives and continued fossil fuel expansion. With record-breaking temperatures, extreme weather events, and the systemic weakening or failure of monitoring systems, the ecological bases of the planet are at threat. Further, the Bulletin observes the information war driven by extractive and predatory technological business models, commodifies human attention and supercharges disinformation through generative artificial intelligence (AI), thereby undermining the foundations necessary for collective risk management. Disruptive technologies, especially AI, are being integrated into military decision-making and weapons systems while also enabling

industrial-scale disinformation, creating unprecedented vulnerabilities in command, control, and democratic oversight.

Geopolitically, the rise of 'winner-takes-all' competition is evident in the Russia–Ukraine war, US–China rivalry, and militarised border clashes in the Middle East and South Asia. The Bulletin accordingly judges the global security situation to be unacceptably high.

The ecological dimension of this polycrisis is documented by the Planetary Health Check, a comprehensive scientific review led by the Stockholm Resilience Centre and the Potsdam Institute for Climate Impact Research. Building on the planetary boundaries framework, this assessment tracks nine global processes that regulate the stability and resilience of the Earth system. By late 2025, seven of these nine boundaries, including climate change, biosphere integrity, land-system change, freshwater change, biogeochemical flows, novel entities, and ocean acidification, had been breached, indicating that humanity is already operating far outside a 'safe operating space' for civilisation.

Across the planetary boundaries, the trends are uniformly negative except for stratospheric ozone depletion and aerosol loading. This is largely due to the success of the Montreal Protocol, while aerosol loading is regionally problematic, especially in South Asia. Climate change indicators continue to worsen, with atmospheric carbon dioxide concentrations exceeding 420 parts per million, increasing radiative forcing, and amplifying extreme weather events. Novel entities, including persistent organic pollutants, plastics, and synthetic chemicals, are accumulating globally with largely unknown long-term impacts. The increasing distance from safe boundaries correlates with exponentially rising unpredictability in Earth-system responses, making cascading failures more probable. These cascading failures translate into complicated security shocks, with simultaneous agricultural crises, mass displacement, and domestic instability.

National strategies and interstate cooperation have progressed at a glacial pace compared to the swiftly degrading ecosystems. The Global Resources Outlook 2024 reports that global resource extraction has tripled over the past five decades and, without urgent intervention, it could increase by another 60 percent by 2060. However, institutional responses remain trapped in a Westphalian paradox where the environmental crisis is global in both cause and consequence, while legitimate political authority remains largely national and fragmented.

The tension between global cooperation and national sovereignty forms the central obstacle to effective environmental governance. States often view international regulations as infringements on their authority to manage resources. Demand for critical minerals such as lithium, cobalt, and rare earth elements, which are essential to the energy transition, has triggered a new form of geopolitics over access and control. The dominance of China over rare earth production and processing, reportedly controlling around 80 percent of supply chains, has prompted the United States and European Union to adopt resource-nationalist strategies, including the US Inflation Reduction Act and the EU Critical Raw Materials Act. These policies prioritise

secure supply chains over global environmental justice, often accelerating green extractivism in the Global South at the expense of indigenous rights.

Given this geopolitical competition, securitisation of resources has emerged as the need of the times. By framing resource scarcity and planetary boundary transgression as existential threats to humanity, securitising actors can claim legitimacy for measures that would otherwise be politically or economically unacceptable. This reframing has two important consequences. First, it aligns environmental and resource governance with the core mandate of safeguarding state survival, making inaction politically costly. Second, it compels security institutions to engage with Earth-system science and socio-ecological resilience as central components of strategic planning rather than as peripheral concerns.

First, any move toward comprehensive resource securitisation must therefore confront the risks of emergency politics. Advocates of resource and climate securitisation argue that the epic is now entering its crisis phase, as signaled by the Doomsday Clock's 85-second setting and the breach of the ocean acidification boundary in 2025. This suggests the need for redefining existing conceptions of emergency that are temporally extended but normatively constrained. In light of these tensions, the breach of a planetary boundary or crossing of agreed resource-use thresholds should trigger a predefined sectoral emergency response, similar to a Public Health Emergency of International Concern (PHEIC) in global health governance. This would mean integrating ecological indicators into early-warning systems and contingency planning.

Second, states would need to nationalise or otherwise improve the strategic resilience of critical infrastructure and resource flows. This does not necessarily imply blanket state ownership but does require comprehensive planning for operational continuity in water, energy, food, and minerals. These measures must be designed to avoid displacing environmental and social burdens onto rural, indigenous, or otherwise marginalised communities.

Our security thinking must integrate the materiality of critical infrastructures and Earth-system processes rather than treating security purely as a discursive construct. In practice, this means that ministries of defence and foreign affairs must develop in-house scientific advice so as to co-design policies with scientific institutions. The choice presented by the 85-second setting is not merely between different policy instruments but between incompatible conceptions of security. If national security communities continue to operate within the traditional paradigms, treating the planetary breaches as far from reality, they risk presiding over the orderly management of decline.

Sruthi Kalyani *is a senior research officer with the Emerging and Deep Tech vertical at CNSS. Her research interests include China's Artificial Intelligence strategy, emerging technologies in international affairs, human rights and technology governance, and critical security studies.*

Genomic Data Sovereignty in India: Cybersecurity Risks to National Biosecurity

Sanjana V

India is in the midst of a genomic revolution. National initiatives such as the IndiGen Programme and the Genome India Project (GIP), alongside emerging hospital biobanks and a rapidly growing direct-to-consumer (D2C) genetic testing market, are generating vast troves of highly sensitive genomic data. Yet this data is being accumulated in an environment where cybersecurity practices are uneven, consent and privacy frameworks remain underdeveloped, and the legal regime treats genetic information largely as ordinary personal data. In this context, *genomic data sovereignty*, the ability of the Indian state and its communities to control how genomic information about its population is collected, stored, accessed, and used, has become a core biosecurity concern rather than a narrow data protection issue.

Genomic data sovereignty poses significant challenges for India amid its expanding genome initiatives, hospital biobanks, and private genetic testing sector. Cybersecurity risks, including cyber theft, foreign access, and misuse of population-level genetic data, threaten national biosecurity due to gaps in data protection, cloud hosting, and cross-border flows. Some of these concerns are discussed in this article.

Hacking DNA Threats

Genomic technology faces cyber vulnerabilities at every stage of DNA sequencing, from sample preparation to data analysis. Hackers exploit networked instruments and poorly secured software to steal or manipulate data, enabling identity tracing, surveillance, or even embedding malware in synthetic DNA strands. Artificial intelligence amplifies these risks by altering genomic datasets, potentially corrupting research, or misguiding medical treatments.

India's major public genomic programmes illustrate both opportunity and vulnerability. The IndiGen Programme, led by the Council of Scientific and Industrial Research, has produced whole-genome sequences for over 1,000 Indian individuals. The Genome India Project, initiated in 2020 by the Department of Biotechnology, has now made genomic data for 10,000 individuals publicly accessible, with the long-term aim of creating an 'Indian reference genome' to support precision medicine and disease research. Data from these initiatives is routed to the Indian Biological Data Centre (IBDC), which serves as the country's first dedicated life sciences data repository. However, legal and ethical frameworks have not kept pace. While the Indian Council of Medical Research (ICMR) has informed consent guidelines, these do not adequately address the specificities of genomic data, long-term secondary uses, and community-level harms. Consent processes often remain one-off and static rather than dynamic, limiting participant agency over future analyses.

Genomic Security in Medicine

Personalised medicine relies on secure genomic data, yet bioinformatics tools are built on outdated code that lacks basic

protection like encryption. Cyberattacks can lead to re-identification attacks, where anonymized data links to individuals via public database or social media. In India, hospital biobanks and private firms like those offering D2C test compound this, with inconsistent practices risking donor anonymity and discrimination. Cloud hosting exacerbates these issues, as third-party services increase unauthorised access risks through misconfigured APIs (Application Programming Interface) or weak controls. From a sovereignty perspective, perhaps the most critical question is *where* Indian genomic data resides and *who* can access it. India's emerging data protection framework has historically been silent or fragmented on genomic data, focusing instead on generic sensitive personal data. Experts forecast stricter genomic privacy under DPDPA, but exemptions for research and compliance gaps persist. Initiatives like Gujarat's 2025 tribal genome project sequence 2000 samples without tailored safeguards. Global trends urge encryption, anomaly detection, and privacy by design, yet India's frameworks lag behind GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act). Cross-border transfers demand government-approved schemes, but localisation mandates raise costs for firms. Multinationals face restructuring, potentially slowing innovation.

India's Cyberattack Risks

India encounters heightened cyberattacks on critical infrastructure, including biomedical sectors. In 2022, ransomware hit the All India Institute of Medical Sciences (AIIMS), compromising data for about 40 million patients, disrupting services like appointments. Russian hackers used phishing to target health ministry sites, stealing employee and physician data across hospitals. By the end of 2026, threats would evolve to AI-driven hyper–personalized phishing and mobile malware, targeting digital ecosystems with genomic relevance. Chinese state-backed attacks on Serum Institute and Bharat Biotech sought vaccine data for a competitive edge, signaling biosecurity motives.

2026 Digital Ecosystem Threats

Predictions for 2026 highlight strategic cyber operations against India, including genomic targets amid biotech growth. Social engineering tactics that uses AI to craft tailored attacks, exploiting data from breaches. Precision medicine biobanks lack regulations, hindering secure data sharing while enabling misuse like genetic discrimination. Foreign access risks rise with cloud reliance, where attackers exploit supply chains for exfiltration. National biosecurity suffers if population genetics, unique to India's diversity, fuels bioweapons or surveillance by advisories.

Protecting India's Genomic Sovereignty

India's genomic future sits at a crossroads. On one path lies a model where genomic data is treated as a largely technical asset, governed by generic data protection rules and fragmented sectoral norms, leaving it vulnerable to cyber-attacks, foreign exploitation, and domestic misuse. On the other hand lies a sovereignty-conscious, cyber-biosecure vision that recognises genomic information as a strategic national and communal resource. At this juncture, India's legal and policy frameworks must explicitly recognise genomic data as a special category that warrants heightened protections, including stricter consent requirements, stronger limits on secondary

uses, and more robust breach notification and redress mechanisms tailored to the irreversibility and familial nature of genetic information. This should be operationalised through a dedicated genomic protection framework that embeds principles of genomic justice, community participation, and fair benefit-sharing, while also strengthening de-identification practices, dynamic consent infrastructures, and the governance capacity of ethics committees and data access bodies.

Further, India must treat genomic infrastructures as critical national assets within a broader cyber-biosecurity strategy, rather than as ordinary research IT systems. National repositories such as the Indian Biological Data Centre, large hospital biobanks, and emerging D2C genomics platforms should be subject to mandatory, independently audited cybersecurity baselines that cover encryption, secure APIs, strong authentication, incident response, and resilient cloud configurations. At the same time, cross-border data transfers and foreign cloud dependencies should be governed by genomic-specific safeguards and rigorous audit mechanisms, while public engagement and genomic literacy initiatives build societal trust. Only by integrating cybersecurity, biosecurity, and human rights into a coherent genomic sovereignty agenda can India harness the benefits of its genomic revolution without compromising the security and dignity of its citizens.

Sanjana V *is a biotechnology student at MS Ramaiah University of Applied Sciences (MSRUAS), interested in science communication, bridging the gap by simplifying complex science for everyone. She is currently an intern at the Emerging and Deep Vertical, Centre for National Security Studies, MSRUAS. She is keen to explore data analytics and data science applications in biotechnology, as well as opportunities in biotechnology management that bridges science and strategy.*

Weaponising Interdependence: China's Rare Earth Export Controls and India's Industrial Dilemma

Arshia Bose

On 9 January 2026, reports emerged that China had begun restricting exports of heavy rare earth elements and powerful magnets containing them to Japanese companies, following Beijing's earlier decision to ban exports of dual-use items that could contribute to Japan's military capabilities. Although framed as a targeted national security measure, the new controls reach well beyond the defence sector, affecting Japan's wider manufacturing base, from automotive components to advanced electronics. Within days, the United States convened a ministerial meeting of key partners and allies, including India, to push for diversification of critical mineral supply chains and to reduce collective dependence on Chinese refining and processing. These developments are the latest expression of a longer arc of the transformation of China's rare earths sector from a low-cost, environmentally damaging resource industry into a strategic export control regime that shapes global industrial hierarchies.

Traditionally, export control regimes have referred to multilateral, consensual agreements between major supplier countries to regulate and control the export of sensitive goods, technologies, and software. This is done to prevent the procreation of Weapons of Mass Destruction and ensure the responsible exchange of goods. The Wassenaar Arrangement, the Nuclear Suppliers Group, and the Missile Technology Control Regime represent this model where these agreements coordinate national licensing systems so that advanced technologies are traded under shared rules, minimising the risk that exports will fuel destabilising military assets. China's recent rare earth export control operate differently, yet effectively function as a de facto export control regime. In current settings, China has begun to restrict exports of rare earths and powerful magnets containing them to Japanese companies. These apply mostly to Japanese industries and are not limited to the defence industry. Asia's top two economies have been embroiled in their biggest dispute in years. Since April and October 2025, Beijing has imposed two waves of controls on rare earth elements and related technologies, formally citing national security grounds and responding to new U.S. tariffs. The first round introduced licensing requirements on seven heavy rare earth elements and associated compounds, metals, and magnets. The second expanded the list to five more rare earths and, crucially, extended controls to technologies and foreign-made goods containing even trace amounts, as low as 0.1 per cent by value, of Chinese-sourced materials or products made using Chinese rare earth technologies.

In today's tense geopolitical environment, rare earths are vital to the manufacturing of a wide range of products, from smartphones to wind turbines. China's ability to weaponise rare earths is the product of decades of deliberate industrial strategy rather than a contingent monopoly. In 2024, China accounted for at least 60 per cent of the world's rare earth production. According to China, these controls were implemented due

to security interests, including protecting resources, controlling critical supply chains, gaining influence in trade negotiations, and consolidating its own supply chain. China, being the world's single largest supplier of the component that is imperative to the manufacturing of the most powerful motors that are used for many applications, leaves the global supply chain highly vulnerable to disruptions.

An alternate approach to understanding China's reasoning behind this is that by managing its exports, China gets to control the rate of industrialisation and development of all the countries that heavily depend on China. China's maximalist approach to manufacturing gives it the ability to cultivate trade dominance over Western nations and their allies. China is slowly moving up the global value chain as manufacturing at an advanced level requires heavy access to these rare earths. Its dominance rose after environmental and economic factors shut down production of rare earths elsewhere.

This can also be seen as a form of quiet economic pressure. It is easier to express export controls as a regulatory process, unlike sanctions. This makes retaliation more difficult and allows pressure to be applied without accountability. Gatekeeping also helps in determining who can innovate the next generation of technologies. Controlling the production of next-generation technologies is one of the most efficient ways of indirectly controlling the global hierarchy. Modern systems are defined by technological capability and are the foundation of power. Eventually, this leads to interdependence in tech supply chains. By doing this, China also stays in the top by creating a form of political hierarchy. This is because when a country is dependent on another, to avoid any form of conflict, it slowly starts aligning its policies with that country. This works in favor of China.

We can look at this situation as a way of China reversing resource hierarchies that have been established in the past. In the past, resource-rich countries would export at a low price while importing expensive finished goods. By deliberately restricting exports at key moments, introducing price floors, and using quotas, China has, at various times, created a two-tier pricing structure in which domestic users enjoy lower input costs than foreign competitors. This enables Chinese firms to move up the value chain into high-tech manufacturing while foreign producers face higher costs and greater uncertainty.

Another key non-traditional aspect that contrasts with the above in some ways is that China is actually a system manager, and not a weaponiser. Rather than pursuing outright bans, Beijing has tended to use licensing, administrative delay, and regulatory ambiguity to shape flows dynamically. The case-by-case licensing system allows it to calibrate pressure, rewarding compliant or strategically important partners while signalling costs to those it seeks to deter or coerce.

Where does India stand with all this?

India is relatively well-endowed with rare earth resources, holding an estimated 6.9 million tonnes of reserves, that is the third-largest globally. In practice, it remains heavily dependent on Chinese imports for permanent magnets and other processed rare earth products used in electric vehicles, white goods, defence systems, and conventional automotive components. Recent export licensing frictions have already led to delays

in approvals for Indian component makers, prompting the domestic automotive industry to warn of risks to production continuity and to urge the government to open urgent diplomatic channels with Beijing.

Beyond magnets, China's restrictions on exports of germanium and other critical materials have raised concerns in India's semiconductor, fibre-optic, and solar sectors. Rapid growth in domestic demand for clean energy technologies and electric mobility implies a sharp increase in the need for critical minerals and rare-earth-intensive components. Yet, India currently lacks large-scale refining and advanced magnet manufacturing capabilities. Environmental concerns, legacy legal constraints, and technological gaps have also slowed the development of a robust domestic ecosystem.

India has begun to respond to these structural vulnerabilities. The National Critical Mineral Mission, backed by a multi-year budgetary allocation, aims to enhance exploration and recycling of critical minerals, reduce import dependence, secure mineral assets abroad, and develop domestic processing technologies. The government is working with Indian Rare Earths Ltd and other public sector entities to accelerate domestic resource development, and is exploring partnerships with resource-rich partners such as Australia for access to rare earth deposits.

There are also indications of a more targeted industrial policy. Proposals for a production-linked incentive (PLI) scheme focused on rare earth magnets and critical mineral recycling are under discussion, and the government has reportedly approved or is considering support packages for magnet manufacturing and allied segments. These moves align with a broader emphasis on selective industrialization that is prioritising sectors such as semiconductors, defence manufacturing, and critical mineral processing, where capability gains can generate strong spillovers and where dependence on concentrated foreign suppliers poses strategic risk.

Building an end-to-end rare earth value chain, from environmentally and socially acceptable mining to separation, alloying, and high-performance magnet fabrication, takes decades, substantial capital, and sustained technological learning. Environmental safeguards and regulatory capacity must be strengthened to avoid reproducing the ecological harms seen in earlier rare earth booms elsewhere. How effectively India navigates this transition will help determine not only its position in global supply chains but also the degree of strategic autonomy it can exercise in an era where export control regimes increasingly shape the contours of global order.

Arshia Bose *is a B.Sc. student in Economics, Mathematics, and Statistics at Mount Carmel College, Bengaluru, with experience across research, consulting, and community-focused initiatives. She has interned at ICRISAT and Publicis Sapient, developing strengths in financial analysis, data visualization, and content analytics.*

*****

Disclaimer

The views expressed by the authors are personal and not to be attributed to the Centre for National Security Studies (CNSS) or MS Ramaiah University of Applied Sciences (MSRUAS). No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from CNSS, MSRUAS. Written request for permission should be emailed to cnss@msruas.ac.in.