



# VANTAGE POINT

A Newsletter on Non-Traditional Security

November 2025



## *Contents*

Resurgence of Avian Influenza in 2025: A Renewed Challenge to Global Biosecurity .....	1
National Security and Economic Stability in the Digital Age .....	3
Jobs and Skills for the Green Economy: Building Human Capital for a Just Transition .....	6
Speaking the Language of Cyberspace: Norms, Attribution and the Crisis of Trust .....	9

# Resurgence of Avian Influenza in 2025: A Renewed Challenge to Global Biosecurity

*Kashvi A*

Avian influenza commonly known as bird flu, has long been recognized as a formidable biosecurity threat with the potential to disrupt global health and food systems. Since June 2025, highly pathogenic avian influenza (HPAI) strains, especially the H5N1 subtype, have re-emerged with a significant surge of outbreaks reported across North America, Europe, and parts of Asia. The United States and Canada have seen [the largest poultry culls](#) in recent years with millions of birds sacrificed in an effort to contain the virus. In Europe, several countries are grappling with widespread [outbreaks in both industrial poultry farms](#) and wild bird populations, complicating containment efforts. Meanwhile, parts of Asia continue to report endemic presence of diverse HPAI strains contributing to the virus's genetic mixing in avian reservoirs.

Genomic surveillance has revealed ongoing mutations in these strains, including alterations in the [hemagglutinin and neuraminidase proteins](#) which enhance the virus's binding affinity to avian respiratory and intestinal cells. Some mutations also suggest increased affinity for receptors found in mammalian respiratory tracts, raising concerns about cross-species transmission potential. This genetic evolution facilitates more efficient spread among bird populations and presents a looming risk of zoonotic spillover to humans. Sporadic human cases linked to recent outbreaks have already been documented emphasising the public health threat.

The economic impacts on the poultry industry have been profound. Beyond the immediate loss of millions of birds, trade restrictions, supply chain disruptions and consumer fears have contributed to a sharp increase in poultry product prices globally. These outbreaks threaten not only food security but also the livelihoods of farmers and communities dependent on poultry farming. The 2025 avian influenza resurgence, therefore, represents a multifaceted biosecurity challenge requiring coordinated animal health, public health, and environmental interventions.

Besides, the 2025 resurgence of HPAI has exposed significant biosecurity challenges that complicate containment and mitigation efforts worldwide. One of the primary difficulties lies in the virus's continuous evolution. Mutations in key viral proteins have enhanced its capacity to spread efficiently among domestic and wild bird populations. Wild birds, particularly migratory waterfowl, act as natural reservoirs and vectors enabling the virus to travel across continents during migration seasons further complicating containment measures on farms and in the environment.

Surveillance and reporting gaps remain a critical issue hampering timely detection and response. In many regions inconsistent monitoring of wild bird populations and limited testing resources delay outbreak identification. This lag can result in extensive viral dissemination before containment protocols activate. Smaller or resource-limited farms often struggle with

implementing standard biosecurity measures such as controlled access, disinfection protocols or isolation of new stock, increasing vulnerability to infection.

Perhaps the most alarming challenge is the risk of zoonotic spillover. While human cases of HPAI remain rare, genetic changes in circulating strains suggest increased affinity for receptors in mammalian respiratory tracts elevating the threat of cross-species transmission. The potential for the virus to adapt for sustained human-to-human transmission raises pandemic concerns, underscoring the urgency of fortifying biosecurity at the animal-human interface.

Addressing these biosecurity challenges requires a holistic approach, such as strengthening wild bird surveillance, enhancing farm-level biosecurity compliance through training and resources, improving data sharing between animal health and public health sectors and maintaining readiness to rapidly isolate and control outbreaks. Only through integrated and coordinated efforts can the evolving threats of avian influenza be effectively managed to safeguard animal and human health.

In response to this ongoing threat, policymakers and international organisations have [strengthened biosecurity frameworks aimed at improving early detection](#), rapid response and containment capacities. Enhanced genomic monitoring of avian

influenza viruses globally allows better tracking of mutations and spread patterns. Investment in next-generation vaccines and antiviral agents is accelerating aiming to protect both avian and human populations. Cross-sector collaboration under One Health initiatives emphasizes the interconnectedness of environmental, animal, and human health in biosecurity planning.

However, implementation gaps remain, particularly in resource-limited settings where infrastructure for disease surveillance and biosecurity enforcement may lag. Continued investment in farmer education on best practices, rapid reporting mechanisms and support for sustainable poultry production models is essential. International cooperation on data sharing and coordinated response is more critical than ever to prevent localized outbreaks from escalating into global crises.

The 2025 avian influenza resurgence is a stark reminder that biosecurity must continuously evolve to meet emerging challenges posed by mutating viruses, global trade and ecological factors. Strengthening integrated surveillance, enhancing biosecurity measures across all levels of poultry production and fostering international collaboration are key to reducing the risk of future outbreaks and protecting both food security and public health.

***Kashvi A** is a B.Sc. (Hons) Biotechnology student currently interning at the Emerging Technologies vertical of CNSS. Her work focuses on research and writing related to bio-warfare, emerging biothreats, and their national security implications.*



## National Security and Economic Stability in the Digital Age

*Sanjana V*

It is needless to say that national security is closely linked to the country's economic stability. National security is inseparable from a country's capacity to maintain economic viability, attract investment, sustain productive capacity, and build resilient infrastructure. The stability and protection of resources, critical infrastructure, and financial systems have become the foundation upon which military capabilities themselves rest. Without a functioning economy, a state cannot acquire the resources necessary for defence, maintain the technological edge required for deterrence, or provide the social stability that prevents internal fragmentation.

India's economic stability in relation to national security has significantly evolved over the years. In the past, India primarily focused on conventional military defence and faced economic vulnerabilities due to limited integration between economic policies and security measures. The two frameworks, security and economics, were treated as separate issues requiring distinct bureaucratic machinery and strategic planning. This compartmentalization reflected historical circumstances and institutional path dependencies. The asymmetry was particularly pronounced in advanced technologies where India remained dependent on imports, foreign expertise, and technology licensing arrangements that placed Indian firms in subordinate positions. Over the past decade, however, a fundamental reorientation has occurred. Today, India is assured to be the world's [fourth largest economy by 2025](#), reflecting

robust growth, strong consumer markets, and strategic government interventions that link economic strength with national security. Economic security is now considered a core pillar of India's defence strategy, emphasized self-reliance in defence production and technological innovation, reducing dependence on imports and boosting defence exports.

India recorded its [highest-ever defence production](#) of ₹1.54 lakh crore in fiscal year 2024-25, with indigenous defence production reaching ₹1,27,434 crore, representing more than triple the level achieved in 2014-15. This surge in domestic production reflects a strategic shift toward [Atmanirbharata, self-reliance](#), as an organising principle for national security. The government has systematically utilised procurement policy to incentivize domestic production, offered preferential terms to indigenous manufacturers, and invested in the development of specialised industrial clusters for defence production. India now exports defence equipment to more than one hundred states.

Cyber security and the protection of critical supply chains from disruption have become integral components of this emerging framework of integrated economic and national security policy. In the digital age, most national economies depend fundamentally on digital infrastructure for banking, communications, manufacturing coordination, government functions, and the management of complex supply chains spanning multiple continents. A disruption to

digital infrastructure ripples instantaneously across the economy in ways that physical destruction does not.

Cyber threats, such as data breaches, ransomware attacks, and espionage, can severely disrupt these economic activities while simultaneously compromising military capabilities and intelligence operations. Unlike traditional military threats that operate primarily at the state level and above and that are constrained by geography and logistics, cyber threats can originate from state actors with sophisticated resources, criminal organisations operating for profit, or non-state groups motivated by ideology or grievance, creating what scholars term [security in ambiguity](#) where attribution is contested and appropriate response is unclear. A cyber operation conducted by a criminal enterprise might create the same damage as one conducted by a state actor, yet the appropriate response differs entirely.

The case of Japan's experience with the sophisticated cyberespionage campaign attributed to the Chinese hacking group [MirrorFace](#) illustrates these dynamics. Between 2019 and 2024, over two hundred cyberattacks targeted Japan's Foreign and Defense Ministries, space agency (JAXA), and major technology firms engaged in aerospace, semiconductors, and advanced manufacturing. Investigations conducted by Japan's National Police Agency and the Cabinet Cyber Security Center linked these attacks to *MirrorFace*, a China-affiliated advanced persistent threat group that employed malware delivery mechanisms and spear-phishing emails to steal sensitive defence technology and national security secrets. The campaign evolved strategically

over time. Between 2019 and 2023, [MirrorFace conducted an elaborate phishing campaign](#) targeting a wide range of critical entities, including think tanks, government agencies, political figures, and the media, aiming to establish persistent presence in valuable networks. The attacks were designed to deliver malicious software that granted unauthorized access to sensitive systems and enabled exfiltration of valuable data over extended periods. On the economic side, the theft of intellectual property from technology firms and aerospace companies weakened Japan's capacity for innovation and damaged global competitiveness precisely in the sectors where Japan had positioned itself as a technology leader.

The lesson learnt is that a vulnerability in a civilian telecommunications network can compromise military communications. A theft of technology secrets from a private company can undermine the competitive advantage that the state had been cultivating as part of its economic strategy. This integration remains inadequate in most governments. effective integration of cybersecurity with broader frameworks of economic and national security requires policies that deliberately establish cyber laws and regulations to protect critical data from both criminal and hostile state actors, encourage public-private partnerships to enhance threat intelligence sharing where private firms report attacks they experience and government shares strategic threat information with private firms, invest in cyber workforce training and awareness programs at scale to build human capacity for defense, and build resilient digital infrastructure capable of withstanding sophisticated cyberattacks through

redundancy, encryption, and rapid response mechanisms.

India has begun moving in this direction with increasing urgency. [The National Cyber Security Reference Framework](#) launched in 2023 aims to enhance defenses against cyber threats, promote secure technology use, strengthen incident response capabilities, and foster indigenous technological innovation in cybersecurity. The government has allocated ₹10,000 crore over five years for enhancing national capabilities through the [IndiaAI mission](#), recognising that cyber resilience is not a luxury or a technical afterthought but rather a prerequisite for economic stability and national security. The Indian government has established the [National Critical Information Infrastructure Protection Centre \(NCIIPC\)](#) to coordinate defence of critical infrastructure across sectors.

The tension between security and openness creates persistent dilemmas without obvious resolution. Economic growth depends on openness to international trade, technology transfer, cross-border flows of capital and talent, and integration into global supply chains where production occurs across multiple countries. Yet this openness creates exposure to espionage, intellectual property theft, supply chain vulnerabilities where

disruption at a single node propagates throughout the entire system, and technological dependence on foreign suppliers who may be adversaries or whose firms may be compromised by adversaries.

The interaction between national security, economic stability, and cybersecurity is complex and vital. National security underpins economic security by providing a safe environment for investment and growth. Economic strength is essential for sustaining defence and security capabilities. Cybersecurity represents the modern frontline; without it, neither economic prosperity nor national security can be assured.

Policy frameworks integration conventional security, economic policy, and country's resilience against emerging threats while enabling sustained economic growth. The future will require sustained commitment to building indigenous technological capacity, strategic partnerships with trusted international actors where mutual benefit can be attained.

***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.*

## Jobs and Skills for the Green Economy: Building Human Capital for a Just Transition

*Sruthi Kalyani*

The transition to a green and low-carbon economy is now framed by climate policymakers and international institutions as one of the most significant economic transformations of our century. Yet, amid discussions of renewable energy infrastructure and emissions reduction targets, a critical aspect of how people who will build, operate, and live through this transition has been relatively overlooked in most of the climate dialogues. A people-centered approach to the green transition is not merely a moral imperative rooted in social equity or human rights. It is fundamentally an economic imperative. Without deliberate investment in human capital, skills development, and inclusive employment pathways, the technological achievements of the green transition will remain stranded investments, unable to be deployed at scale or sustained over the long term.

Most national climate action strategies prioritise technological infrastructure while allocating minimal resources to the development of the human resource needed to install, and innovate within these new systems. This imbalance threatens to undermine the entire climate transition, creating a scenario where the tools for decarbonisation exist but cannot be fully utilised because of the lack of skilled workforce.

A [recent research](#) from Systemiq and the World Resources Institute (WRI) reveals that the climate transition could create an estimated 375 million new jobs over the next

decade, with adaptation activities, building resilient infrastructure, drought-resistant agriculture, and climate-proofing urban areas, generating an additional 280 million jobs worldwide. This represents a significant economic opportunity, with a 20 percent increase in employment in the renewable energy, construction, and nature-based solutions sectors. However, [fewer than 50 percent of national climate plans](#) incorporate training strategies for upskilling workers in green economy opportunities. This means that even as governments commit to expanding renewable energy capacity and transitioning away from fossil fuels, the majority have not undertaken the necessary institutional planning to ensure that workers can access and succeed in the jobs being created. In the renewable energy sector alone, the absence of adequate vocational training could result in a shortage of six million skilled workers by 2030.

The skills shortage in renewable energy carries implications that extend far beyond individual employment outcomes or corporate competitiveness. Labour shortages in the power sector would delay the rollout of renewable energy capacity, leaving global renewable generation nearly 10 percent below pledged targets by 2030. This cascade of consequences would drive power sector emissions to 12 percent above 2030 pledges and more than double them by 2045, effectively placing the 1.5 C warming target permanently out of reach.

Climate negotiations have progressively recognised the centrality of jobs and skills to

climate action, yet this recognition has remained largely rhetorical and bereft of concrete mechanisms for implementation. At COP28 in Dubai in 2023, climate change language for the first time explicitly mentioned “skills development among young people” to promote green job opportunities, marking a symbolic acknowledgment that the transition cannot proceed without deliberate workforce development. However, this language remained aspirational rather than operational. The same COP28 session also formalized the [Just Transition Work Programme \(JTWP\)](#), which was initially established at COP27, aiming to address workforce concerns in climate negotiations by incorporating dialogues on workers’ rights and the participation of affected communities. The JTWP represented a structural innovation in climate governance: for the first time, a dedicated institutional mechanism explicitly focused on the social dimensions of climate transition rather than treating labor issues as secondary considerations within broader climate policy discussions. The programme’s explicit recognition of labour rights, social protection, and social dialogue was celebrated by international labour organizations and worker representatives as a historic breakthrough. Yet at COP29 in Baku in November 2024, despite further highlighting skills shortages as barriers to climate implementation, negotiating parties did not launch concrete global mechanisms for skills mobilisation or workforce development. The Work Programme remained largely consultative, convening discussions and issuing recommendations without establishing binding commitments, dedicated financing

mechanisms, or accountability structures that would ensure implementation.

Critically, labour unions and worker organisations that are the very actors with the understanding of workforce capacity, training infrastructure, and worker transitions, have been largely excluded from substantive climate negotiations, leading to justified skepticism about what constitutes genuinely just and inclusive transitions. While the JTWP includes participation from worker representatives, their influence on actual climate policies remains limited, and negotiating parties have consistently failed to translate worker input into binding institutional commitments. The International Trade Union Confederation (ITUC) and affiliated worker organisations have consistently demanded that governments [prioritise the full implementation of the Just Transition Work Programme](#) with explicit commitments to skills development, social protection, and labour rights enforcement. Without binding legal language, financial allocations, or enforcement mechanisms, these demands have remained exhortations rather than requirements.

This implementation gap led to the launch of the [Global Initiative on Jobs and Skills for the New Economy](#) at COP30 in Belém on November 12, 2025, representing a deliberate attempt to move beyond rhetoric toward concrete coordination and action. Developed in collaboration with the COP30 Presidency and a coalition of international partners, the Initiative brings together governments, businesses, civil society organisations, labour unions, and philanthropic actors around a shared workforce transition strategy. Unlike previous climate initiatives focused primarily



on technology transfer or renewable energy capacity, this Initiative explicitly treats human capital investment as central to climate action rather than as an ancillary concern.

India's engagement with global green initiatives and its position on green jobs and skills development reflects the particular constraints and opportunities facing large developing countries attempting to conduct rapid energy transitions while addressing poverty and employment challenges. India has committed to the Global Initiative, emphasising that skills development cannot proceed without adequate climate finance from developed nations. India's renewable energy achievements are undeniably impressive, [The country has reached 50 percent of its installed electricity capacity from non-fossil fuel sources](#), achieving its 2030 NDC target five years ahead of schedule, and is on trajectory to [install 500 gigawatts of non-fossil capacity by 2030](#), making it one of the few G20 nations on track to meet or exceed its Paris Agreement commitments. This achievement reflects the success of government initiatives, including the [Pradhan Mantri KUSUM](#), the PM Surya

Ghar scheme, and the National Wind-Solar Hybrid Policy, which have generated employment at scale while expanding energy access. Yet scaling renewable energy to create genuinely inclusive employment requires capacity-building support, technology transfer, and concessional financing from developed nations to train workers, develop supply chains, and establish the institutional infrastructure for a just skills-to-jobs transition.

There is an urgency of building the green economy workforce. The logic is circular and reinforcing. Without workers trained in renewable energy installation and maintenance, renewable capacity cannot be deployed at planned scale, and without deployment at planned scale, energy sector emissions shall keep increasing. This reality creates an opportunity for transformative change. The scale of investments required for green workforce development, if mobilised now, could establish human capital as the foundation for sustainability, positioning countries that invest in workers and skills as the winners of the green economy transition.

***Dr. Sruthi Kalyani** is a Senior Research Officer with the Emerging and Deep Technologies Programme at the Centre for National Security Studies (CNSS). Her research focuses on China's artificial intelligence strategy, emerging technologies in international affairs, human rights and technology governance, and critical security studies.*

## Speaking the Language of Cyberspace: Norms, Attribution and the Crisis of Trust

*Manisha S*

In the twenty-first century, cyberspace has evolved from being a merely a domain of technological innovation into a central arena of global politics. As states increasingly rely on digital infrastructure for governance, economy, and security, their exposure to cyber risks has greatly struck up and also there are intriguing imposal of threats. The consequences are no longer theoretical. Cyberattacks cascade across borders in seconds, causing economic devastation, destabilizing governments, and holding societies hostage. Cybersecurity has transcended its technical origins to become a new diplomatic practice itself. Yet the emerging framework of cyber diplomacy remains fragmented and contested language and its limitations is essential for thinking through how global order might be sustained in an era of digital conflict.

The strategic significance of cyberspace cannot be overstated. The [Stuxnet operation](#) of 2010, widely attributed to U.S. and Israeli intelligence agencies, demonstrated that cyber operations could cross the threshold between the virtual and the physical, destroying tangible infrastructure and causing measurable harm to nuclear facilities. By targeting Iran's uranium enrichment centrifuges at Natanz through industrial control systems, Stuxnet illustrated that cyberattacks were no longer confined to information theft or network disruption but could inflict the kind of direct physical damage traditionally associated with military conflict.

Today, critical infrastructure worldwide faces persistent targeting. Germany's nuclear power plants, India's electrical grids, and American water treatment facilities have all been targeted by reconnaissance missions and intrusion attempts from state and non-state actors. NATO recognised this evolving threat landscape by designating cyberspace as an operational domain in 2016, placing it on equal footing with air, land, and sea warfare. By 2021, the alliance had made clear that a sufficiently destructive cyberattack could trigger Article 5, the collective defense clause that treats an attack on one member as an attack on all. This strategic shift has created three fundamental diplomatic challenges that cyber norms must address, namely, the question of sovereignty, the problem of power projection without traditional military means, and the crisis of trust between actors operating in a domain where attribution remains technically contested and politically manipulated.

Cyberspace, unlike physical territory, recognises no borders. Malicious traffic can originate from one state, route through proxies across multiple continents, and strike targets thousands of miles away in microseconds. How states exercise control over digital attacks without admitting either their complicity or their inability to govern their own networks is critical to the conduct of their statecraft. Simultaneously, cyberspace has democratised destructive capability. A state with limited military spending can project disproportionate

power through cyber means. North Korea, Iran, and Russia have demonstrated that cyber capabilities allow smaller players to strike major powers with relative impunity, creating asymmetric deterrence dynamics. Underlying these tensions is a fundamental crisis of trust, when perpetrators can be masked through false-flag operations, states find it difficult to build confidence in their mutual commitments to restraint.

The rise of cyber diplomacy represents an attempt to address these challenges through institutional frameworks and diplomatic mechanisms. Cyber diplomacy operates through multiple channels, including the development of international norms of responsible state behavior, the establishment of confidence-building measures between adversaries, the creation of mechanisms for attribution and signaling, and the negotiation of binding legal instruments. The United Nations has emerged as the primary venue for norm-setting, hosting both the [Group of Governmental Experts \(GGE\)](#) and the [Open-Ended Working Group \(OEWG\)](#) to negotiate frameworks for responsible state conduct. The [Budapest Convention](#), the first binding international legal instrument addressing cybercrime, entered into force in 2004 and has since been ratified by 81 states, creating harmonised approaches to investigating cybercrimes and enabling cross-border law enforcement cooperation. Further, regional frameworks have supplemented these global efforts. For instance, the OSCE has developed sixteen confidence-building measures focused on transparency and information-sharing, while the [African Union's Malabo](#)

[Convention](#) provides a regional legal framework for cybersecurity governance.

Yet for all these institutional achievements, cyber diplomacy remains profoundly challenged by structural obstacles hindering emerging consensus. Attribution, despite advances in forensic capability, remains fundamentally contested. Unlike nuclear weapons or conventional military operations, cyber operations can be masked through false-flag tactics, tool-sharing networks, and sophisticated layering of infrastructure. Different states maintain different evidentiary standards for attribution, making international consensus difficult. Misattribution, on the other hand, can cause irreversible damage to diplomatic relationships or lead to military escalation based on faulty intelligence.

The second major challenge is the endemic hypocrisy that undermines norm-setting efforts. The states most vocally championing cyber norms are the ones among those most actively conducting offensive cyber operations. The U.S. National Security Agency had classified the phrase “[offensive cyber operations](#)” for years. Revelations from the Snowden archive documented extensive U.S. cyber espionage capabilities targeting allied nations. China has been credibly attributed to sustained campaigns of intellectual property theft and critical infrastructure reconnaissance. Russia has conducted numerous cyberattacks against Baltic states, France, and other nations, while simultaneously promoting UN resolutions against cyber aggression. This contradiction of preaching norms while practicing violations creates a credibility deficit that

undermines the legitimacy of the entire norm-setting enterprise.

The multistakeholder nature of cyberspace creates diplomatic complications that state-centric frameworks struggle to accommodate. Not all states possess equivalent cyber capabilities. Wealthy nations with advanced technical expertise and infrastructure investment, such as the United States, China, Russia, Israel, and a small number of European nations, can conduct sophisticated cyber operations and attribute attacks with precision. Most nations lack these capabilities, making them disproportionately vulnerable and leaving them dependent on more powerful states for threat intelligence and defensive assistance. This creates perverse incentives where weak states may choose not to publicly attribute attacks precisely because they cannot independently verify attributions or respond if their attributions prove incorrect.

Capacity-building initiatives, while valuable, risk becoming vehicles for geopolitical influence, as wealthy states use technical assistance to extend their diplomatic reach into less developed regions. The UN's emphasis on confidence-building measures and information-sharing assumes that all states have an equivalent capacity to implement these measures, but a developing nation may lack the infrastructure even to maintain points of contact or participate in joint exercises.

Despite these challenges, cyber diplomacy represents progress within severe constraints. The consensus around protecting the public core of the internet reflects shared recognition that certain infrastructure deserves special protection.

The Budapest Convention, despite its limitations, has harmonised cybercrime legislation across diverse legal systems. Joint attribution by multiple states, while controversial, creates diplomatic accountability that would otherwise be absent. What remains imperative is acknowledging that cyber diplomacy cannot solve problems that are fundamentally technological or strategic in nature through diplomacy alone.

The path forward demands institutional innovation. States should establish dedicated cyber diplomacy units within foreign ministries, staffed with technologists and security experts alongside traditional diplomats, to bring genuine expertise to negotiations. The future of cyber diplomacy will ultimately be determined by whether states can sustain cooperative frameworks despite deep geopolitical competition. The current moment shows both promise and peril. On the one hand, states have demonstrated an unprecedented willingness to engage in diplomatic processes regarding cyberspace, and a consensus around certain norms has emerged. On the other hand, the gap between professed norms and actual behavior widens, and technological change threatens to outpace diplomatic adaptation. The emergence of AI, quantum computing, and other advanced technologies will create new forms of threat that existing frameworks are ill-equipped to address. If cyber diplomacy is to remain relevant, it must develop mechanisms for rapid norm revision, create forums for discussing emerging technologies before they become vectors for conflict, and build institutions that can adapt as the technological



landscape shifts. This is not a challenge that any single state or diplomatic forum can address alone. It demands sustained, multilateral cooperation.

***Manisha S** is an undergraduate pursuing BSc biotechnology at Ramaiah University of Applied Sciences, focused on community health and well-being. She is interested in researching on the intersection of health, research and social impact. Currently an intern at the Emerging Tech Vertical at CNSS, she is passionate towards contributing initiatives promoting preventive healthcare and enhancing public awareness through evidence-based approaches.*

\*\*\*\*\*

*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](mailto:cnss@msruas.ac.in).*