

MP-IDSA *Issue Brief*

25 Years after Amerithrax: The Changing Landscape of Biosecurity

Aayushi Sharma and Ajey Lele

September 18, 2026

Summary

The 2001 anthrax attacks in the US led to the emergence of biological terrorism as a public health, law enforcement, intelligence, and national security problem, highlighting the need for an integrated approach to addressing the threat. Advances in biotechnology, synthetic biology, and emerging technologies have defined the biological threat landscape over the past 25 years.

Introduction

The deadly attacks of 11 September 2001 were followed by another critical terrorist incident in the United States, wherein anonymous letters laced with the deadly anthrax spores were sent to several media companies and post offices. The attacks claimed the lives of five people through the inhalation of anthrax and infected several others who came in contact with the postal envelopes. The Federal Bureau of Investigation (FBI) codenamed the investigation ‘Amerithrax’.¹ The ‘Amerithrax Task Force’ was created to determine the source of this terrorist attack. The FBI subsequently released an ‘Amerithrax Investigation Report’ detailing the course of the investigation.² The investigation focused primarily on scientists associated with the US biodefence establishment, especially the US Army Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland.

The investigation subsequently went through a series of phases which were deemed controversial. Several scientists were designated as ‘persons of interest’ and came under surveillance and investigation. In several cases, the suspects also pushed back against the allegations of deliberately releasing anthrax. One known suspect, Steven Hatfill, a pathologist and a biological weapons expert, ultimately received a large government settlement after pursuing legal action over being falsely accused in connection with the attacks.³ In 2008, another biodefence scientist, Bruce Ivins, a senior biodefence researcher at USAMRIID who was identified as the principal suspect, died by suicide.⁴ The FBI formally closed the investigation in 2010, concluding that Ivins was the actual culprit and that he had acted alone. However, an independent scientific review found that the evidence was consistent with Ivins being the culprit, but still inadequate to conclusively establish his responsibility.⁵

Along with the rapid investigations, the anthrax attacks also triggered a major national public health and law enforcement response, widespread disruption to postal services, and extensive decontamination efforts. Executed only a week after one of the worst terrorist attacks in modern history, the anthrax attacks added to the already heightened threat perceptions regarding terrorism. As a result of these attacks, biological terrorism emerged as a public health, law enforcement, intelligence, and national security problem, highlighting the need for an integrated approach to addressing the threat. Biological terrorism or bioterrorism, however, was not a novel phenomenon. There have been numerous accounts of non-state actors

¹ [“Amerithrax or Anthrax Investigation”](#), Federal Bureau of Investigation.

² [“Amerithrax Investigation Report”](#), *The New York Times*, 19 February 2010.

³ [“Scientist Officially Exonerated in Anthrax Attacks”](#), *The New York Times*, 8 August 2008.

⁴ Gregory Frederick, [“A Review of The Mirage Man: Bruce Ivins, the Anthrax Attacks, and America’s Rush to War”](#), *Journal of Microbiology & Biology Education*, Vol. 12, No. 2, pp. 211–212.

⁵ [“Timeline: How the Anthrax Terror Unfolded”](#), *National Public Radio (NPR)*, 15 February 2011.

using or attempting to use hazardous biological materials as weapons to create widespread harm.⁶

This brief addresses response mechanisms, bio-surveillance, and emerging technology challenges to contextualise where the world stands today on bio-preparedness, 25 years after the 2001 Anthrax attacks. It explores the critical implications and opportunities for the Biological Weapons Convention (BWC) in shaping the future of global biosafety and biosecurity. The brief evaluates how two-and-a-half decades of science, technology, and policy evolution have shaped our preparedness against biological and toxic threats, and the challenges that persist.

Biodefence and Response Mechanisms

Response mechanisms and biodefence are a critical interdisciplinary field focused on protecting human life and agriculture. Key organisations involved include laboratories studying biological science, agricultural research centres, medical sciences, public health agencies, pharmaceutical companies, and national security agencies. Over the last 25 years, states worldwide have developed specific agencies associated with biological threats. Some states have developed advanced biodefence strategies and institutional mechanisms, while others are still working on them. It is also important to recognise that this threat has always been dynamic, so continued attention is required when deciding on response mechanisms and biodefence practices.

When it comes to addressing the risks posed by biological weapons, it is important to focus on the unique characteristics and vulnerabilities regarding biological agents. These agents include infectious pathogens and biotoxins that are non-transmissible. These weapons often have delayed effects and variable incubation periods, which add to the challenges of building robust response mechanisms for such threats. The case of anthrax attacks in the US made it fundamentally clear that investigations into biological weapons attacks are often met with attribution challenges. The challenge of effective attribution persists and is often exacerbated by rapid advances in biotechnology and easily accessible biological design tools.

The fragmented nature of biological weapons dissemination also challenges preparedness and response. While in the US, anthrax spores were dispersed through the postal mail, such agents can also be disseminated through aerosols or even contamination of important resources such as crops or water supplies, causing widespread damage. Therefore, as these threats rapidly evolve, delivery mechanisms

⁶ Stephan Riedel, [“Biological Warfare and Bioterrorism: A Historical Review”](#), *Baylor University Medical Center Proceedings*, Vol. 17, No. 4, 2004, pp. 400–406.

for such agents are easily accessible to non-state actors, further complicating attribution.

The 2001 anthrax attacks exposed massive vulnerabilities in the public health detection and response systems, intelligence gathering, and inter-agency coordination mechanisms in the US. The US hence worked to build national capacities through the Public Health Security and Bioterrorism Preparedness Act of 2002 to strengthen prevention, preparedness, and response mechanisms against biothreats and to develop stringent standards for securing dangerous biological agents. The Act also imposed strict regulations on the possession, use, and handling of specific biological agents. To build on these response capabilities, Congress enacted the Project BioShield Act in 2004, which incentivised companies to research, develop, and stockpile medical countermeasures against CBRN threats.⁷ Incentivising research in medical countermeasures also heightens capabilities to address novel bio-risks and leverage technological advancements to improve detection and response mechanisms.

Globally, funding surged for biodefence and preparedness research, as well as for high-containment facilities, to build scientific, defence, and policy capabilities to counter such threats.⁸ The preparedness gaps to deal with bioterrorism threats were significantly highlighted in the aftermath of the anthrax attacks. The World Health Organization (WHO) developed the International Health Regulations in 2005 to legally require signatory countries to build national capacities for detecting, analysing, and surveilling public health emergencies of international concern.⁹

Additionally, the Global Health Security Initiative (GHSI) emerged in 2001 as a cross-regional multilateral grouping to improve cooperation in public health preparedness mechanisms to respond to CBRN terrorism threats, with WHO as the technical advisor.¹⁰ The anthrax attacks thus led to growing attention on improving biodefence, international coordination in public health preparedness, and response capabilities, not just within the US but worldwide.

Thus, in 2001, bioterrorism emerged as a pressing challenge requiring coordination across public health, national security, and law-and-order agencies. However, contemporary issues relating to emerging technologies, AI integration, dual-use research of concern (DURC), and the evolving capabilities of biotechnology are creating new pathways to biological misuse and redefining the biosecurity landscape.

⁷ [“Project BioShield”](#), Administration for Strategic Preparedness and Response.

⁸ Carrie M. Long and Andrea Marzi, [“Biodefence Research Two Decades Later: Worth the Investment?”](#), The Lancet Infectious Diseases, 1 August 2021.

⁹ [“International Health Regulations”](#), World Health Organization.

¹⁰ [“Global Health Security Initiative: 10 Years of Collaboration in Action”](#), European Commission, 2011.

Bio-Situational Awareness and Intelligence Gathering Mechanisms

One of the most effective ways to address novel threats is to build robust disease surveillance systems that track unusual occurrences that may signal a public health emergency. Disease surveillance is therefore a key pillar of early recognition and detection. Bio-surveillance essentially involves gathering and analysing relevant data to provide periodic information on biological threats affecting human, animal, plant, and environmental health. Strong bio-surveillance systems build bio-situational awareness and early detection, improving national and global capacities to address bio-risks.

Various approaches may be used to develop such systems, such as syndromic surveillance, which involves gathering data through public health officials reporting on suspected threats based on the reported symptoms of a given population, or event-based surveillance, which involves a wider range of information systems involving newspaper reports, social media, or publicly reported incidents.¹¹ Epidemiological studies have also become central to early detection by understanding disease patterns and transmission.

However, the anthrax attacks revealed that public health surveillance may not only deal with accidental bio-risks but also deliberate attacks. The resulting policy shift led the US to treat biological risks as a national security problem. The Department of Homeland Security created the BioWatch system as a direct result. BioWatch served as an early-warning system to detect the aerosolised release of certain pathogens through a network of sensors.¹²

Gathering public health data and developing bio-situational awareness is beneficial not only in the context of deliberate biothreats but also accidental ones. Therefore, even after 25 years of terrorist attacks using anthrax, efforts are underway to develop global bio-surveillance mechanisms to build transnational capacities to tackle such threats. Integrated bio-surveillance efforts would require simultaneous data collection from several sources, including public health institutions, high-containment laboratories, pharmacies and wastewater facilities.¹³ Current efforts extend surveillance beyond public health data to include animal, plant, and environmental health. This One Health approach to bio-surveillance and intelligence

¹¹ Natasha E. Bajema, William Beaver and Christine Pathemore, [“Toward a Global Pathogen Early Warning System: Building on the Landscape of Biosurveillance Today”](#), Council on Strategic Risks, 20 July 2021.

¹² [“The BioWatch System”](#), in *BioWatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats*, National Academies Press, 2011.

¹³ Vijey Nema, [“Biosurveillance”](#), *Microbial Diversity in the Genomic Era*, 2019.

gathering requires active global cooperation frameworks that go beyond national implementation.¹⁴

To build global coordination mechanisms, organisations like the WHO have worked to develop early warning detection systems and transnational response systems to address the threats posed by pathogens with pandemic potential. WHO has several initiatives, including the International Pathogen Surveillance Network (IPSN) and the Global Outbreak Alert and Response Network (GOARN), which provide technical coordination to identify and respond to public health emergencies.

The Epidemic Intelligence from Open Sources Initiative (EIOS) and the WHO Hub for Pandemic and Epidemic Intelligence also provide technical assistance to countries to improve detection and monitoring capabilities.¹⁵ While these initiatives exist, building an integrated approach to intelligence sharing and data gathering, along with inter-agency coordination, such as the World Organisation for Animal Health (WOAH) and the Food and Agriculture Organization (FAO), for a One Health framework remains a challenge.

Translating these bio-surveillance capabilities into effective early warning systems also comes with its own set of nuances. For global early warning systems to work well in deliberate and accidental disease outbreaks, capacities need to be built towards interoperable systems capable of operating in diverse demographic and geographic settings.¹⁶ One major driver of continued efforts to build better, more integrated bio-surveillance, early warning, and detection systems is the increased perception of biological risk in recent years. Even after more than two decades of anthrax attacks, the challenge of keeping biological weapons capabilities out of the hands of non-state actors persists due to the novel risks posed by artificial intelligence (AI) as well as developments in biotechnology.

Emerging Technologies: Boon and Bane

Rapid advances in biotechnology, synthetic biology, gene editing, AI and related technologies are strengthening biodefence while simultaneously lowering barriers to biological misuse. Developments in biotechnology continue to offer immense potential to enhance biological defence capacities by supporting research into rapid

¹⁴ Nithin Ramakrishnan, [“Bio-surveillance as One Health: A Critique of Recent Definitions and Policy Initiatives”](#), *Development*, Vol. 66, 2023, pp. 215–225.

¹⁵ [“International Pathogen Surveillance Network”](#), World Health Organization; [“The Global Outbreak Alert and Response Network”](#), World Health Organization; [“Epidemic Intelligence from Open Sources \(EIOS\)”](#), World Health Organization; [“The WHO Hub for Pandemic and Epidemic Intelligence”](#), World Health Organization.

¹⁶ [“Global Early Warning System: Safeguarding Against Future Pandemics”](#), Food and Agriculture Organization of the United Nations.

detection, diagnosis, and improved medical countermeasures, including vaccine development and other prophylactic treatments. Advances in life science research capabilities have also expanded the potential of gene sequencing methods such as metagenomic sequencing to provide simultaneous, independent analysis of the total genetic material in a sample.¹⁷

Biotechnology developments, when considered alongside accessible AI integration, also present opportunities to improve drug discovery, vaccine development, and other pharmaceutical interventions. AI models can also help with biological data analysis, as well as structuring and synthesising large databases to support research. Targeted attention is also being paid to improving medical measures against drug-resistant bacteria and viruses through frontier AI models along with improved gene editing capabilities.¹⁸ Therefore, a case can be made for responsible and governed use of AI in biotechnology and life science research. This integration could help address longstanding concerns and improve the biosecurity landscape.

While the opportunities presented by AI and biotechnology are widely recognised, they are also accompanied by concerns about potential risks, especially in the absence of integrated governance and regulatory frameworks. Improvements in biotechnology capabilities over the years have also created space for faster, cheaper, and more accessible DNA synthesis technologies, driving market expansion among DNA synthesis providers. However, screening protocols for ordered DNA sequences have not been implemented to the same extent.

These capabilities require structured, standardised, and uniform screening regulations to verify customer identities comprehensively. These regulations are crucial for ensuring that DNA sequences of potentially dangerous pathogens are only provided to legitimate research facilities with adequate institutional biosafety standards in place. Currently, DNA providers primarily belong to the International Gene Synthesis Consortium, a commercial group of providers in the global market.¹⁹ The Consortium has established the Regulated Pathogen Database (RPD) to verify given orders and detect the sequences of concern.²⁰

They may either conduct customer screening to establish the identity of the ordering parties or screen the sequences ordered to identify potentially dangerous and controlled pathogens or biotoxins. However, without a legal mandate within the

¹⁷ Torsten Thomas, Jack Gilbert and Folker Meyer, “[Metagenomics - A Guide from Sampling to Data Analysis](#)”, Microbial Informatics and Experimentation, 9 February 2012.

¹⁸ Amir Elalouf, Hadas Elalouf, Ariel Rosenfeld and Hanan Maoz, “[Artificial Intelligence in Drug Resistance Management](#)”, *Biotech*, Vol. 15, No. 5, 2025.

¹⁹ [International Gene Synthesis Consortium](#).

²⁰ Tanya Sarawagi and Suryesh K. Namdeo, “[The Double Helix of Danger: Securing Synthetic DNA in India](#)”, Occasional Paper, Observer Research Foundation, 27 August 2026.

Consortium, screening DNA synthesis orders before fulfilment is largely voluntary. This staggered safeguards landscape creates gaps in screening and contributes to biosecurity concerns about unregulated access to hazardous biological materials.

The integration of AI into this biotechnology landscape therefore adds another layer of complexity. While certain frontier AI models may be instrumental in synthesising large datasets to aid biological research, they may also lower technical thresholds, especially open-source large language models (LLMs), by disseminating information on biological design.²¹ A study auditing 32 LLMs found that most complied with requests to design and generate novel toxin sequences.²² Similarly, recent scientific research shows that generative AI models can develop genome sequences for novel viruses that target bacteria resistant to natural bacteriophages.²³ This development also raised concerns about diverting these capabilities to engineer drug-resistant, human-infecting viruses.

Safeguards on the end of AI developers also become significant in this case. Anthropic’s newer models have safety classifiers in place, with evaluations conducted on refusal benchmarks to assess the models’ ability to handle prompts related to the hazardous use of biological weapons.²⁴ However, despite these mechanisms, Anthropic’s recent threat assessment report revealed several attempts to bypass the safety classifiers and retrieve questionable information on gene editing of infectious pathogens and toxin design.²⁵ Thus, in the context of deliberate biotreats, greater access to bio-design tools and open-source AI platforms equipped with the requisite knowledge are among the most pressing challenges in the current global biosecurity discourse.

Strengthening Global Norms for Biosecurity

Biosecurity is a crucial pillar of the international security architecture. Considering the broad spectrum of biological risks, ranging from natural and accidental outbreaks to deliberate weaponisation of infectious pathogens and biotoxins, the global norms on biosecurity are embedded in various institutional mechanisms.

²¹ [“Redefining Biological Weapons: Expanding the BWC to Incorporate Infrastructure Harm and Cyber-Biothreats”](#), Nuclear Threat Initiative, 20 November 2025.

²² Shu Quan, Tianfang Hao, Sitong Fang, He Geng, Jiayi Zhou, Boyuan Chen, Kaile Wang, Donghai Hong, Juntao Dai, Yaodong Yang and Jiaming Ji, [“A Blind Spot in Alignment: Quantifying Biosecurity Risks in Large Language Models”](#), arXiv, 5 August 2026.

²³ Samuel H. King, Claudio L. Driscoll, David B. Li, Daniel Guo, Aditi T. Merchant, Garyk Brix, Max E. Wilkinson and Brian L. Hie, [“Generative Design of Bacteriophages with Genome Language Models”](#), *Science*, Vol. 393, No. 6811, 2026.

²⁴ [“Why Do We Take LLMs Seriously as a Potential Source of Biorisk”](#), Anthropic, 5 September 2025.

²⁵ [“Detecting and Countering misuse of AI: September 2026”](#), Anthropic, 10 September 2026.

Major international frameworks on deliberate biothreats include the Biological and Toxin Weapons Convention (BTWC) and UNSCR 1540, while the WHO sets norms for public health issues such as biosafety standards, disease surveillance, detection, preparedness, and response mechanisms. The voluntary export control groupings such as the Australia Group are significant in managing transnational trade in controlled substances with relevance to chemical and biological weapons.

The ‘biological weapon taboo’, or the perceptions against the use of biological materials as weapons, was recognised through the prohibition of use under the 1925 Geneva Protocol.²⁶ This development was further strengthened and legally enforced through the Biological and Toxin Weapons Convention (BTWC), which entered into force in 1975.²⁷ While the BTWC has largely succeeded in establishing the norm against biological weapons, contemporary challenges relate to enforcing these norms through practical frameworks that adequately address emerging risks.

The Convention legitimises the use of biological materials for peaceful life science research while prohibiting any use not intended to be peaceful. In theory, this may seem like a significant qualifier for what the regime permits and prohibits. However, questions and uncertainties arise as the dual-use characteristics of life science research and subsequent AI integration in biotechnology take shape.

With frontier AI models, scientists are increasingly studying capacity-building in medical countermeasures to address drug-resistant pathogens, which requires careful use of gene-editing technologies. However, the same capabilities can also be diverted towards more lethal use of genetically engineered pathogens for harmful purposes. Therefore, without international verification mechanisms, determining the legitimacy of biological research for peaceful purposes becomes a mammoth challenge for the existing regime.

Current structural challenges in the Convention also include the lack of a Science and Technology Advisory Body to monitor and routinely conduct a scientific review of the treaty. This development would be necessary to adequately assess the Convention’s capacity to address emerging biosecurity risks. The ongoing working group discussions to strengthen the Convention are a significant step forward in this regard. The Convention’s scientific capacities can also be enhanced by developing networks of high-containment laboratories with strong biosafety standards.

The Organisation for the Prohibition of Chemical Weapons (OPCW) has provided a precedent for such a structure, with designated biomedical and environmental

²⁶ Phillip M. McCauley and Roger A. Payne, “[The Illogic of the Biological Weapons Taboo](#)”, *Strategic Studies Quarterly*, Vol. 4, No. 1, 2010, pp. 6–35.

²⁷ Bakhtiyar Tuzmukhamedov, “[Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological \(Biological\) and Toxin Weapons and on their Destruction](#)”, Audiovisual Library of International Law, 10 April 1972.

facilities also in place.²⁸ Such a network for the BTWC could facilitate independent, regulated research into sequencing novel pathogens and toxins to develop stronger verification mechanisms for the treaty. Building effective regulatory practices without infringing on or curtailing scientific progress is a pressing challenge for the BTWC.

Alongside laboratory security measures, research verification, international cooperation and compliance, efforts to prevent misuse by non-state actors are also significant to strengthening global biosecurity norms. The anthrax attacks of 2001 widened the perceptions around biosecurity to include the threats posed by non-state actors as well as inadequate regulatory oversight of research facilities. Hence, stronger norms backed by practical frameworks are essential for improving biosecurity in response to bioterrorism threats.

Deliberations at BWC review conferences signal a careful yet staggered recognition of the threat of bioterrorism. The final declaration of the seventh review conference of 2011, for the first time, condemned terrorism ‘in all its forms and manifestations’ in the context of using biological agents, further highlighting the role of UNSCR 1540.²⁹ In the absence of verification and implementation mechanisms for the Convention, instruments such as UNSCR 1540 and its oversight mechanism through the 1540 Committee provide important frameworks for advancing global security protocols against bioterrorism.³⁰

Given the plethora of emerging challenges surrounding synthetic biology, open-source AI models, and rapidly evolving biotechnology capabilities, institutionalising appropriate safeguards and building an integrated approach is essential to strengthening biosecurity normative frameworks.

While the anthrax attacks presented a case of deliberate use of biotoxins to inflict harm, hence a biological weapons attack, the experience of COVID-19 presented the need to consider pandemic preparedness and response as an international security issue.³¹ Many response and biodefence capabilities that support defence against accidental biothreats and natural outbreaks also support defence against deliberate threats. Thus, lessons should be learned from the COVID-19 pandemic of 2020, and the institutional inadequacies that hindered global coordination should be addressed to build international capacity.

²⁸ [“Designated Laboratories”](#), Organisation for the Prohibition of Chemical Weapons.

²⁹ [“Final Document of the 7th Review Conference: 7th Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological \(Biological\) and Toxin Weapons and on Their Destruction”](#), United Nations Digital Library, 5–22 December 2011.

³⁰ [“Resolution 1540 \(2004\)”](#), Resolution, United Nations Security Council, 28 April 2004; [“1540 Committee”](#), United Nations Security Council.

³¹ Saskia A. Rutjes, Iris M. Vennis, Edith Wagner, Vakhtang Maisaia and Lukas Peintner, [“Biosafety and Biosecurity Challenges During the COVID-19 Pandemic and Beyond”](#), *Frontiers in Bioengineering and Biotechnology*, 1 March 2023.

Conclusion

The anthrax attacks of 2001 revealed that mitigating biological threats requires an integrated approach towards bringing together public health, law enforcement, bio-surveillance and national security frameworks. Twenty-five years later, amid a rapidly advancing emerging risk landscape, the reality remains the same. The COVID-19 pandemic of 2020 is particularly significant in this regard. The pandemic exposed gaps in current detection and preparedness capabilities and underscored that global biodefence mechanisms must support robust, transnational early detection and response.

Developments in biotechnology, synthetic biology, gene editing, and AI models offer immense opportunities to advance life science research. Still, they also heighten concerns about access to biological materials, lowered technological thresholds, and deliberate misuse. While AI integration in biotechnology cannot replace tacit laboratory knowledge, institutions need to strengthen biosafety mechanisms and regulatory oversight to prevent accidental exposure and outbreaks. Similarly, safeguards around DNA synthesis acquisition and screening mechanisms are essential to reduce perceived threats around the availability of controlled and high-risk sequences.

Additionally, effective bio-surveillance mechanisms become important for improving early-warning systems, preparedness, and detection capabilities. While national frameworks for addressing bio-risks exist in practice, existing international frameworks are still essential for building multilateral and transnational capacity against these risks. Efforts are underway to address longstanding issues in the BTWC, especially regarding legally binding verification mechanisms, international assistance and cooperation, and stronger compliance.³² While these developments largely reflect state obligations, continued deliberations on threats posed by non-state actors are also crucial within the Convention.

After more than two decades, the anthrax attacks provide a strong vantage point to evaluate the priorities of the existing biosecurity landscape. The experience of anthrax and COVID-19 indicates that biological threats cannot be treated simply as low-probability possibilities. Sustained investment in prevention, detection, attribution, medical countermeasures, and international cooperation remains essential.

³² [“Ninth Session of the Working Group on the Strengthening of the Biological Weapons Convention”](#), United Nations Office at Geneva, 2026.

About the Author

Ms. Aayushi Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.



Group Captain (Dr.) Ajey Lele (Retd.) is Deputy Director General at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

© Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) 2026