



CENTRE FOR
JOINT WARFARE
STUDIES

GL/30/26

NUCLEAR INNOVATION, DUAL-USE TECHNOLOGIES, AND GLOBAL SECURITY IN THE INDIAN LANDSCAPE

BY

DR HASEEB CHEERATHADAYAN

ORGANISED BY CENJOWS
03 SEP 2026

**BALANCING PROMISE AND PERIL: NUCLEAR INNOVATION, DUAL-USE
TECHNOLOGIES AND GLOBAL SECURITY IN THE INDIAN LANDSCAPE**

BY DR HASEEB CHEERATHADAYAN

ORGANISED BY CENJOWS ON 03 SEP 2026

The presentation examined the dual-use nature of nuclear technology from an Indian security perspective. It highlighted how the same science that powers medicine, energy, industry and research can pose serious threats if radioactive materials or expertise are diverted or misused. Radioactive sources, radiological dispersal devices, nuclear deterrence, emerging technologies and strategic trade controls were discussed. The need for a security architecture covering the entire life cycle of radioactive material was underscored. The session concluded with a call to link healthcare, science, industry, regulators and security agencies into one national nuclear-security system.

The discovery of nuclear fission was cited as the origin of both nuclear power and nuclear weapons. Radioisotopes that diagnose cancer, sterilise equipment and inspect industrial structures can become security concerns if removed from regulatory control. The dual-use dilemma was described as the vast space between peaceful and military uses. Nuclear security was defined broadly to include theft, sabotage, illicit trafficking, cyber compromise and misuse of radioactive material.

India's Nuclear Environment SIPRI data showed about 12,241 warheads held by nine nuclear-armed states in early 2025, with nearly all modernising their arsenals. China's stockpile of around 600 warheads was noted, making India's deterrence environment increasingly triangular. Dual-capable missiles were identified as a source of crisis ambiguity. Artificial intelligence, hypersonic and cyber operations were seen as adding further uncertainty to early-warning and command systems. Dual-use security was therefore presented as a spectrum rather than a fixed category.

Radioactive Sources and Risk UNSCEAR estimates of 40 million diagnostic nuclear-medicine procedures, and 1.4 million radionuclide therapies each year were cited. Most short-lived medical isotopes were described as low risk. High-activity sealed sources in

irradiators, teletherapy and industrial radiography were flagged for greater attention under IAEA categorisation. The point was made that “medical isotopes” do not form a single security category. A risk-informed approach to security was recommended.

Radiological Dispersal Devices A dirty bomb was distinguished from a nuclear explosive, as it disperses radioactive material rather than causing a nuclear blast. Its strategic effects were described as fear, evacuation, economic disruption and loss of public trust. The IAEA Incident and Trafficking Database was cited as evidence that loss and trafficking of radioactive material are real threats. The problem was said to begin long before a device is built. Securing sources across their full life cycle was presented as the best defence.

Hospitals and Industry in National Security Hospitals and industrial facilities were identified as part of the national nuclear-security environment. Every step from delivery to disposal was described as a point where discrepancies must be detected. Technologists, medical physicists, nurses and radio pharmacists were highlighted as a possible first line of defence against diversion. Linking clinical governance with national security, without militarising hospitals, was advocated.

Insider Threats and Security Culture Technology alone was deemed insufficient for nuclear security. Staff were described as both a potential vulnerability and the strongest security asset. Two-person verification, periodic reconciliation, segregation of duties and clear escalation pathways were recommended so that no single error or malicious act could undo the system.

Artificial Intelligence and Digital Security AI were noted for strengthening inventory tracking, surveillance, anomaly detection and customs analysis. The same tools were seen as enabling AI-driven cyberattacks and phishing against facilities, hospitals and suppliers. Human oversight was emphasised, with cyber and physical security treated as one system.

Strategic Trade Controls India’s framework, including the WMD Act 2005 and SCOMET, was outlined along with its membership of the MTCR, Wassenaar Arrangement and Australia Group and alignment with NSG guidelines. Proliferation through small firms,

academic exchange and cloud-based data transfers was flagged as harder to detect. An export-control ecosystem linking government, academia and industry was urged, without stifling innovation.

Nuclear Doctrine and Non-State Threats India's doctrine of credible minimum deterrence and no first use was noted as designed for state-to-state conflict. Radiological terrorism by non-state actors was seen as complicating attribution and response. It was clarified that this does not necessarily signal the end of NFU. Clear response options below the nuclear threshold, supported by nuclear forensics and intelligence cooperation, were recommended.

Recommendations for India A cradle-to-grave digital tracking system for high-risk radioactive sources was proposed. Nuclear-security training for hospitals, universities and industry, and exercises covering theft, cyber compromise and insider scenarios, were urged. Stronger forensic capability, an updated SCOMET framework and closer coordination among DAE, AERB, security agencies, customs, healthcare and industry were also recommended.

Conclusion and Outlook Responsible innovation, rather than fear or complacency, was advocated. India's goal was framed as innovation without proliferation, accessibility without vulnerability and progress without compromising security. The future of nuclear innovation was said to depend not only on what humanity can create, but on how effectively it protects what it creates.