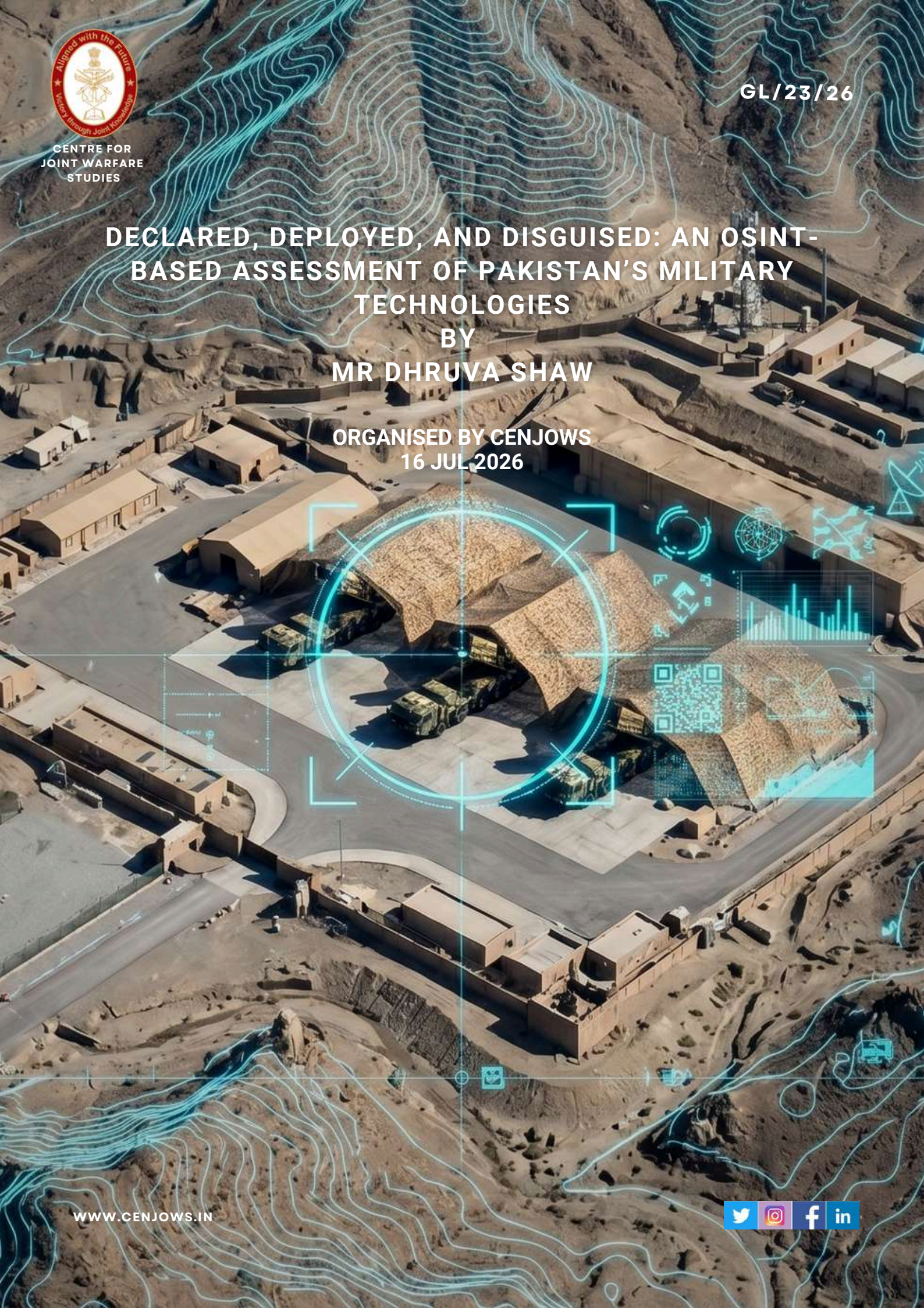

CENTRE FOR JOINT WARFARE STUDIES

GL/23/26

# DECLARED, DEPLOYED, AND DISGUISED: AN OSINT-BASED ASSESSMENT OF PAKISTAN'S MILITARY TECHNOLOGIES

BY

MR DHRUVA SHAW

ORGANISED BY CENJOWS
16 JUL 2026

# DECLARED, DEPLOYED, AND DISGUISED: AN OSINT-BASED ASSESSMENT OF PAKISTAN'S MILITARY TECHNOLOGIES

## BY MR DHRUVA SHAW

## ORGANISED BY CENJOWS ON 16 JUL 2026

The Centre for Joint Warfare Studies (CENJOWS) organised a technical presentation on an Open-Source Intelligence (OSINT) assessment of Pakistan's military technologies, delivered by a Technical Research Assistant with expertise in robotics, automation, cybersecurity, signal processing, and intelligent systems. The session aimed to provide a comprehensive understanding of Pakistan's military capabilities through the systematic use of publicly available information, geospatial intelligence, and open-source investigative techniques. The presentation remained focused on technical analysis and evidence-based assessment, avoiding geopolitical commentary while highlighting the opportunities and limitations associated with OSINT research.

The speaker commenced by outlining his professional background and research contributions, including his work in robotics and intelligent systems, biometric identification technologies, and cybersecurity. His recognition by the IEEE Signal Processing Society through the 2024 scholarship was also highlighted, reflecting his expertise in advanced signal processing and technical research. This introduction established the technical foundation for the subsequent discussion on military intelligence gathering through open-source resources.

The presentation examined Pakistan's military capabilities across multiple domains, including its nuclear programme, missile systems, aerospace modernisation, naval assets, digital tradecraft, and military-related commercial enterprises. Drawing upon publicly available government publications, procurement records, satellite imagery, defence reports, and geospatial analysis, the speaker demonstrated how OSINT can provide valuable insights into strategic military developments. At the same time, he

emphasised the need for careful verification of information due to the presence of misinformation and deliberate information management practices.

A significant portion of the presentation focused on Pakistan's strategic missile and nuclear infrastructure. The speaker discussed the country's medium-range ballistic missile programme, including systems reportedly capable of carrying Multiple Independently Targetable Re-entry Vehicles (MIRVs). Publicly available information was used to identify uranium enrichment facilities, missile testing infrastructure, and suspected nuclear storage locations. Geospatial mapping of selected military installations illustrated the strategic reach of Pakistan's missile capabilities and highlighted the importance of satellite imagery and location-based analysis in assessing defence infrastructure.

The discussion further explored Pakistan's ongoing aerospace modernisation, noting its gradual transition towards a more capable offensive posture through the induction of advanced Chinese-origin fighter aircraft and unmanned combat aerial vehicles. Procurement records and open-source documentation indicated continued investment in both conventional and unmanned aerial platforms, alongside improvements in integrated air defence systems. The speaker also observed that, unlike India's centralised Defence Research and Development Organisation (DRDO), Pakistan's defence research and development activities are distributed across multiple organisations and institutions.

The naval component of the presentation examined Pakistan's expanding maritime capabilities, particularly the acquisition of Chinese-supported submarine platforms and the development of supporting naval infrastructure. Using commercial satellite imagery and publicly available information, the speaker highlighted the increasing militarisation of the Makran Coast through the construction of naval facilities, submarine support infrastructure, coastal defence positions, and logistics installations. These developments were presented as indicators of Pakistan's efforts to strengthen its maritime posture in the Arabian Sea.

Another important aspect of the presentation focused on Pakistan's military-affiliated commercial enterprises and mechanisms employed to sustain defence procurement. The

speaker discussed the role of military-owned organisations operating across sectors such as engineering, logistics, insurance, fertilisers, and ship maintenance. He also explained how shell companies registered in foreign jurisdictions have been identified in publicly available reports as facilitating procurement activities and helping circumvent international sanctions. This assessment illustrated the broader relationship between commercial networks and military capability development.

The presentation also examined Pakistan's radar infrastructure and integrated air defence network through geospatial mapping techniques. Several radar installations and surface-to-air missile deployment sites were identified using satellite imagery and publicly available data, demonstrating how open-source analysis can be employed to monitor strategic military assets. The speaker explained the operational significance of these installations and illustrated how their geographical distribution contributes to national air defence coverage.

In discussing cybersecurity and digital tradecraft, the speaker highlighted both the strengths and vulnerabilities of Pakistan's digital military ecosystem. While several military systems appear to employ robust cybersecurity measures, publicly accessible procurement portals and official government publications were identified as valuable sources of intelligence. The speaker demonstrated how seemingly routine administrative information, when combined with other open-source material, can reveal organisational structures, procurement activities, and military deployments. He also cautioned that publicly available information should always be assessed critically, as open-source environments may contain deliberate misinformation or deception intended to mislead analysts.

During the interactive discussion, the speaker elaborated on the methodologies used in professional OSINT investigations. He emphasised the importance of advanced search techniques, systematic source verification, and the integration of specialised analytical tools for data collection and relationship mapping. Practical insights were shared on the use of digital investigative platforms, interpretation of procurement records, analysis of military order of battle, and exploitation of satellite imagery to develop reliable intelligence

assessments. The methodologies discussed were presented as broadly applicable to the study of military developments in Pakistan, China, and other countries.

The session concluded with an engaging exchange between the speaker and participants, during which questions centred on investigative methodologies, source validation, and the practical challenges associated with analysing military technologies through open-source information. Overall, the presentation provided valuable technical insights into contemporary intelligence gathering, demonstrating the growing importance of OSINT in defence and strategic studies. It reinforced the need for rigorous source verification, multidisciplinary analysis, and responsible interpretation of publicly available information while showcasing the significant role of emerging technologies and digital investigative techniques in modern military intelligence research.