CENTRE FOR JOINT WARFARE STUDIES

GL/22/26

EMERGING PARADIGMS IN DIGITAL FORENSICS: THE INDIAN LANDSCAPE

BY
LT COL (DR) SANTOSH KHADSARE

ORGANISED BY CENJOWS
02 JUL 2026

EMERGING PARADIGMS IN DIGITAL FORENSICS: THE INDIAN LANDSCAPE

BY LT COL (Dr) SANTOSH KHADSARE

ORGANISED BY CENJOWS ON 02 JUL 2026

Lecture Summary

The lecture examined the rapidly evolving domain of digital forensics and its growing importance in addressing contemporary security challenges in the Indian landscape. Lt Col (Dr) Khadsare highlighted how digital forensics has transformed from being a specialised investigative aid into a critical component of criminal investigations, cyber incident response, and national security. With increasing digitisation across society, digital evidence has become central to establishing facts, reconstructing events, and supporting judicial processes.

He explained that the legal framework in India, including the Information Technology Act, 2000, and subsequent amendments, has progressively strengthened the admissibility of scientifically acquired digital evidence. However, the effectiveness of digital investigations depends upon maintaining the integrity of evidence throughout its acquisition, preservation, analysis, and presentation.

The speaker identified several structural challenges confronting India's digital forensic ecosystem. Among the most significant is the absence of a dedicated regulatory mechanism for certifying digital forensic practitioners and standardising professional practices. Unlike the medical or legal professions, digital forensic experts currently operate without a formal accreditation framework, raising concerns regarding quality assurance, professional competence, and consistency in judicial proceedings.

Lt Col (Dr) Khadsare also observed that although digital evidence is increasingly relied upon during investigations, its successful use in courts is often constrained by procedural lapses, technological limitations, and deficiencies in evidence handling. He emphasised that strengthening professional standards and capacity building would significantly improve the credibility and legal admissibility of digital forensic evidence.

Drawing upon real-world case studies, including the Colonial Pipeline ransomware attack and the Pulwama attack, he demonstrated how digital forensic investigations

play a decisive role in reconstructing cyber incidents, recovering encrypted information, tracing digital footprints, and supporting criminal prosecution. These examples illustrated the increasing complexity of modern investigations and the need for specialised forensic capabilities.

A major focus of the lecture was the impact of emerging technologies on digital forensic practices. The transition from conventional hard disc drives to solid-state drives, widespread adoption of cloud computing, Internet of Things (IoT) devices, encrypted communication platforms, and virtualised environments have significantly increased the complexity of evidence acquisition and analysis. Looking ahead, developments in 6G communications, quantum computing, and advanced encryption technologies are expected to pose even greater challenges for investigators.

The speaker underlined the importance of memory forensics, noting that volatile memory often contains critical evidence such as encryption keys, malware artefacts, and live system information that may disappear if not acquired promptly. He stressed that forensic methodologies and tools must continuously evolve to keep pace with rapidly changing digital technologies.

Lt Col (Dr) Khadsare also discussed the capacity constraints facing India's forensic ecosystem. Increasing volumes of digital evidence, expanding numbers of cybercrime cases, significant case pendency in forensic laboratories, and shortages of trained professionals have collectively affected the timeliness and effectiveness of investigations. He advocated greater investment in specialised training, practical skill development, and augmentation of forensic infrastructure to address these challenges.

The lecture further explored the growing role of Artificial Intelligence (AI) in digital forensics. While AI-generated content, including deepfakes and synthetic media, presents new investigative challenges, AI also offers significant opportunities to automate data processing, accelerate evidence analysis, identify relevant artefacts from large datasets, and improve investigative efficiency. The speaker observed that AI would increasingly become an indispensable tool for managing the scale and complexity of digital investigations.

A recurring theme throughout the lecture was the importance of achieving greater technological self-reliance. Lt Col (Dr) Khadsare emphasised the need to develop

indigenous digital forensic tools and technologies to reduce dependence on imported solutions while enhancing national security and technological resilience. He cited ongoing efforts such as the development of Chitragupt as examples of India's growing capability in this field.

Key Takeaways

The lecture highlighted that digital forensics has become an indispensable capability for safeguarding national security, combating cybercrime, and strengthening the criminal justice system. As digital technologies continue to evolve, India must develop a robust and self-reliant digital forensic ecosystem supported by indigenous technologies, modern forensic infrastructure, highly skilled professionals, and a comprehensive regulatory framework. The establishment of professional standards, investment in capacity building, and closer collaboration between government, academia, industry, and law enforcement agencies will be essential to enhancing the country's digital investigative capabilities and ensuring the integrity and credibility of digital evidence in the years ahead.