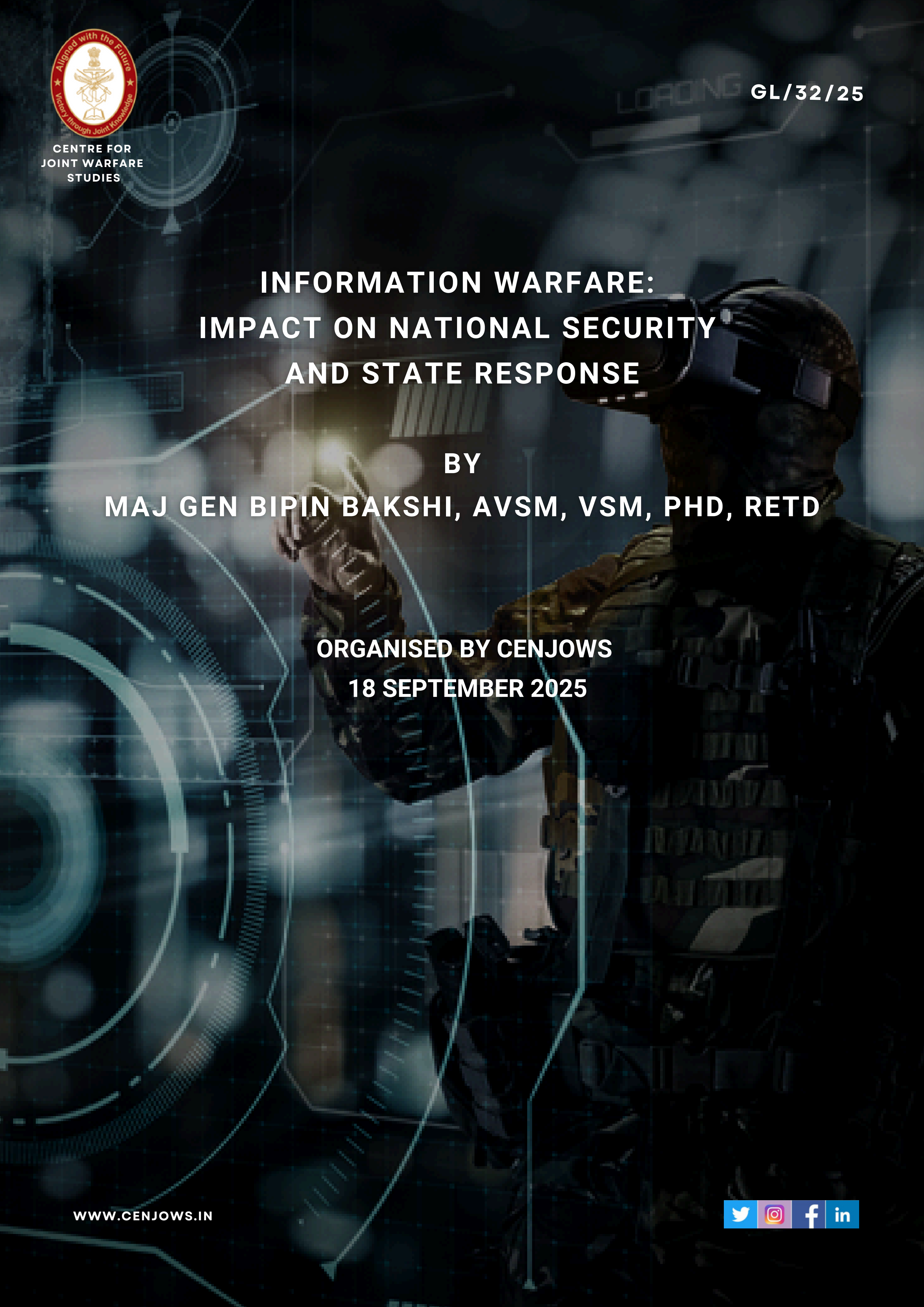

CENTRE FOR
JOINT WARFARE
STUDIES

GL/32/25

INFORMATION WARFARE: IMPACT ON NATIONAL SECURITY AND STATE RESPONSE

BY

MAJ GEN BIPIN BAKSHI, AVSM, VSM, PHD, RETD

ORGANISED BY CENJOWS
18 SEPTEMBER 2025

WWW.CENJOWS.IN

INFORMATION WARFARE: IMPACT ON NATIONAL SECURITY AND STATE RESPONSE
BY MAJ GEN BIPIN BAKSHI, AVSM, VSM, PHD, RETD

ORGANISED BY CENJOWS ON 18 SEP 2025

Contemporary warfare is unavoidably multi-domain, and information and cyber operations are now as critical as the traditional domains of land, air, sea, and space. The basic components of Info Warfare, in accordance with Indian Military publications, are comprised of Psychological Operations, Cyber Warfare and Electronic Warfare. While it is widely understood in theory that cyber operations, psychological operations, and electronic warfare form a single, integrated battlespace, but this has yet to be achieved in practice. Our structures, as well as HR processes for all three services are in distinct silos. Any attempt to treat them as distinct is misguided because adversarial narratives and disinformation penetrate through cyber defences and directly target cognition. In this context, the integration of cyber and psychological operations is crucial for building effective information warfare strategies.

Tracing the evolution of terminology, it becomes clear as to how concepts moved from psychological warfare during the Second World War to “information operations” and “perception management” in the late twentieth century, and eventually to today’s “strategic communications.” Despite changing labels, the substance remains constant: IW is fundamentally a contest over perceptions. What has shifted most dramatically is the speed, reach, and borderless nature of the digital ecosystem. Information flows instantaneously, transcending borders, and often operates outside effective legal regulation. Laws of armed conflict designed for kinetic violence do not cover non-kinetic influence operations, leaving states exposed in a grey zone of continuous hostility.

During recent crises during Operation Sindoor, both India and Pakistan carried out cyber disruptions targeting civilian and administrative systems such as ticketing and welfare platforms. At the same time, gaps in official communication left a vacuum that was filled by speculative media coverage, generating parallel realities that distorted public perceptions. This experience highlighted the necessity of credible and timely communication as an integral part of national defence.

The United States integrates cyber defence with content monitoring under its Cyber Command, conducting “hunt forward” missions abroad and adopting overt doctrines to strike malicious activity at the source. Singapore has created a dedicated Digital and Intelligence Service to institutionalise this integration. Russia’s extensive cyber campaigns in Ukraine were partly neutralised through the combined effects of U.S. Cyber Command’s presence, Microsoft’s cloud support, and Starlink’s satellite connectivity. China has advanced further with its “three warfares” approach, and wide networks of state and militia units are engaged in cyber espionage, with European governments noting a qualitative surge in Chinese capabilities. These examples illustrate that successful responses are continuous, institutionalised, and deeply integrated across technical and cognitive lines.

By contrast, India’s institutional architecture remains fragmented. Moreover, there is a shortage of trained personnel across government, law enforcement, and industry. The absence of a comprehensive national information warfare strategy and a standing strategic communications hub has left India largely reactive.

There is a need for urgent reforms in this regard. The creation of a National Strategic Communication Authority with a permanent, round-the-clock war room to monitor information flows, coordinate across agencies, and issue timely communication is a must. Emphasis should also be given to continuous training and upskilling to ensure that personnel remain capable of addressing the rapid evolution of technology. India should invest not only in defensive capabilities but also in lawful offensive options and counter-disinformation mechanisms.

It clearly emerged that information warfare is a decisive and unavoidable arena of modern conflict. Adversaries today hack minds as much as they hack machines. Unless India integrates its cyber and psychological operations, establishes a central authority to harmonise efforts, and continuously trains its personnel, it risks losing the information battle long before conventional hostilities begin.