“Unmanned aerial systems provide low-cost, deniable capabilities for intelligence collection and precision strikes

Emerging technologies and non state actors: A new emerging threat

by **Vibhuti Thapliyal**

From the rudimentary phishing kits of early jihadist forums to the algorithmically calibrated influence operations of today's AI-driven propaganda bots, cyberspace has emerged as the fifth domain of conflict where violent non-state actors can exert influence far exceeding their material capabilities.[1]

> **"Globally, cyber incidents targeting governments, businesses, and individuals have surged by over 38% in the past year, with state and non-state actors exploiting increasingly sophisticated digital tools to amplify their impact.[2]"**

In contrast to traditional insurgencies, cyber-enabled threats are borderless, capable of traversing sovereign borders in milliseconds while combining the ubiquity of global networks[3].

The 2008 Mumbai attacks, partly enabled by GPS and real-time mobile communications, foreshadowed this convergence of digital and kinetic operations.[4] Today's adversaries have augmented those early methods with a layered arsenal: artificial intelligence to personalise persuasion and optimise attack timing, unmanned aerial systems for reconnaissance and precision strikes, end-to-end encryption to shield command-and-control, and deep social engineering to compromise targets from within.[5]

By eroding public trust, degrading critical infrastructure, and fracturing political cohesion, violent

1 Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. Journal of Military Studies, 4(1), 1–37.
2 GIREM. (2024). GIREM Report. Global Institute for Research on Emerging threats and Markets, p. 17
3 My thanks to Anurag Sharma and Keshav Dhyani for their helpful comments on this article.
4 Rickli, J., & Liang, C. (2024). New and Emerging Technologies for Terrorists. In Routledge eBooks (pp. 118–126).
5 Kaur, H. (2025). The Evolution of Terrorism in the Digital Age: Cyber Jihad and Emerging Threats. International Journal, 14(1[3]), 28–29.

non-state actors (VNSAs) can impose costs on states that far exceed the resources expended. This asymmetry is amplified by the democratisation of technology: the same machine-learning architecture that powers a search engine or recommends consumer products can, with minimal adaptation, be repurposed to craft extremist manifestos or orchestrate disinformation campaigns at scale (Rickli & Liang, 2024, pp. 118–126).

Emerging technologies as force multipliers

AI and machine learning

Violent non-state actors are increasingly leveraging artificial intelligence to enhance propaganda precision and streamline recruitment. Machine-learning algorithms analyse user behaviour to identify ideological vulnerabilities, delivering tailored extremist content across linguistic and cultural boundaries. AI-powered chatbots simulate human interaction, sustaining engagement, radicalising targets, and retaining recruits at scale, at minimal cost and without operational fatigue (Kaur, 2025, pp. 28–29).

Drones and autonomous systems

Unmanned aerial systems provide low-cost, deniable capabilities for intelligence collection and precision strikes. Non-state actors have repeatedly deployed reconnaissance drones in conflict settings (Cohen & Freilich, 2024, pp. 143–148), while ISIS's drone program during the Mosul siege demonstrated how improvised devices can be converted into effective battlefield assets (Rickli & Liang, 2024, pp. 118–126) – capabilities traditionally associated with state militaries.

Encryption and the Dark Web

Encrypted communication platforms such as Signal, WhatsApp, and Telegram shield operational planning from interception, while dark web services facilitate the procurement of explosives, malware, and stolen data[6] (Kaur, 2025, pp. 28–29).

> **"Following post-2015 counterterrorism crackdowns, ISIS migrated significant elements of its propaganda and command infrastructure to anonymised networks, complicating intelligence and law-enforcement penetration.[7]"**

Case study: the Islamic State's cyber caliphate

The Islamic State (IS) provides one of the most instructive models for integrating emerging technologies into insurgent doctrine. Its "Dawn of Glad Tidings" Twitter application enabled decentralised, crowdsourced propaganda dissemination, generating tens of thousands of tweets daily before its removal (Sharma, 2020, pp. 368–391). Following significant territorial losses, IS migrated much of its infrastructure to encrypted communication channels, dark web hosting, and multilingual outreach, including content in Malayalam and Tamil, specifically designed to target Indian recruits.

[6] Cohen, M. S., & Freilich, C. D. (2024). Cyberterrorism. In Routledge eBooks (pp. 143–148).

[7] Sharma, A. (2020). Wilayat-e-Internet: Islamic State Cyber Caliphate. National Security, III–III, 368–391.

The 2014–2015 prominence of the @ShamiWitness account, operated by Indian engineer Mehdi Masroor Biswas, an IS propagandist, demonstrated how a single actor, leveraging anonymity and social media amplification, could become a global propaganda hub with millions of monthly impressions (Sharma, 2020, pp. 368–391). This convergence of technical proficiency, networked amplification, and ideological alignment exemplifies the asymmetric challenge of twenty-first-century counterterrorism.

India's vulnerability and strategic gaps

India confronts a dual strategic challenge: the rapid expansion of its digital economy and critical infrastructure has significantly widened the national cyber-attack surface, while the integration of doctrine and operation across cyber, intelligence, and kinetic domains remains incomplete.[8] Initiatives such as the Defence Cyber Agency (DCyA) and CERT-In represent important institutional progress, yet they lack systematic incorporation of AI-threat analysis, multilingual online monitoring capabilities, and scenario-based cyber wargaming into national security planning.

[8] UNIDIR. (n.d.). Building a More Secure world. United Nations Institute for Disarmament Research.

> **"Current global counterterrorism frameworks insufficiently account for adversarial AI risks, including data poisoning, model backdooring, and the exploitation of algorithmic bias in automated decision-support systems, vulnerabilities that could undermine both tactical operations and strategic stability."[9]**

Conclusion: staying ahead of the curve

The weaponization of emerging technologies by violent non-state actors is no longer a speculative concern; it is an operational constant. From AI-optimised radicalization pipelines to drone-enabled urban warfare, the qualitative leap in capability has already transformed the threat landscape (Rickli & Liang, 2024). For India and its strategic partners, the imperative extends beyond merely hardening technical defences; it requires actively shaping the normative and legal frameworks that govern conduct in this contested digital battlespace.

The states that will prevail are those capable of integrating resilience, anticipatory threat analysis, and proactive diplomacy, denying adversaries not only access to critical systems but also the ability to control the narrative. This entails coupling robust cyber and AI governance with confidence-building measures, ensuring that technological innovation strengthens, rather than destabilizes, the international security order (Lubis, Muttaqin, & Nurwahidin, 2025).[10]

About the Author

Vibhuti Thapliyal is a Master's student in the History and Philosophy of Knowledge at ETH Zürich, where her research draws on science and technology studies (STS), philosophy, and the social sciences to examine emerging technologies, governance, and ethical decision-making. She previously worked with the Vivekananda International Foundation in the Technological and Scientific Studies division on projects focusing on AI-enabled warfare, autonomous weapon ethics, and the geopolitics of defence innovation. Her research interests include the "AI commander problem," accountability in autonomous military systems, and the governance of emerging technologies in hybrid and asymmetric conflict.

9 ENISA. (2023). AI Cybersecurity Guidelines. European Union Agency for Cybersecurity.

10 Lubis, H. A., Muttaqin, M. I., & Nurwahidin, N. (2025). The Cyber Proxy War: Non-State Actors Role in Global Geopolitical Competition. Journal Research of Social Science Economics and Management, 4(6), 815–828.


SYSTEM HACKED