MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Commentary

Technology, Terror and National Security Challenges

Ntogwa N. Bundala

October 08, 2025

Summary

The relationship between technological innovation and violent extremism presents significant national security challenges.

Technology's rapid and unpredictable evolution in today's interconnected world creates a constantly changing environment where state actors and terrorists use new technologies to gain strategic advantages. The relationship between technological innovation and violent extremism presents significant challenges for nation-state security policies, requiring a deep understanding of how technology can empower defenders and aggressors.

Governments have significantly improved their counter-terrorism efforts through advanced technologies that aim to prevent, detect and disrupt terrorist activities. Artificial intelligence and machine learning algorithms now analyse large data streams, spotting suspicious behaviours and potential threats with remarkable accuracy. Surveillance technologies, including biometric identification, facial recognition and extensive data mining, enable real-time monitoring of movements and communications. This is crucial for stopping terrorist plots before they occur.

Cyber capabilities allow states to protect critical infrastructure while conducting offensive operations that weaken terrorist networks' communication and financial systems. Social media monitoring tools and digital counter-narratives further disrupt extremist propaganda and recruitment efforts. These technologies allow states to respond proactively in a domain beyond traditional geographic limits.

Terrorist groups, despite having limited resources, have also become skilled at taking advantage of technological advances. Encrypted messaging apps like Telegram and Signal offer secure, anonymous communication that complicates intelligence work. Social media platforms are used to spread propaganda, recruit members and raise funds globally, allowing groups to connect with audiences far beyond their immediate physical surroundings.

Emerging technologies like affordable drones have been adapted for reconnaissance, targeted strikes and smuggling operations. While their cyber activities are not yet at the same level as state actions, they represent a new front for disruption. Terrorists also use open-source platforms, crowdsourced intelligence, and freely available online guides to refine their tactics and avoid detection. This ability to innovate rapidly turns the digital landscape into a significant force for terrorist activities.

The relationship between technological advancements and terrorist exploitation resembles an arms race. Every new surveillance capability inspires better encryption, while every counter-narrative campaign leads to more subtle propaganda strategies. Nation-state cyber defences push terrorist groups to innovate with social engineering and decentralised networks. This ongoing cycle expands the battlefield into new areas, from cyberspace to outer space, blurring the lines between traditional warfare,

crime and civilian life. The technologies that enable states to act decisively also encourage terrorists to explore new ways to attack, ensuring that this competition is ongoing rather than conclusive.

Using technology in counter-terrorism, for nation-states, presents a dilemma. On one hand, surveillance systems, predictive analytics and digital monitoring have stopped numerous attacks by identifying threats before they happen. On the other hand, these same tools raise issues around privacy, civil liberties and public trust. Communities may feel alienated if they think they are unfairly targeted by intrusive monitoring. For terrorists, technology offers anonymity, speed and reach. Encryption secures their communications, online platforms amplify their ideology, while drones and cyber tools enhance their operational capabilities. States cannot just ban or eliminate these technologies as they are vital for business, communication and daily life.

The answer lies in managing technology’s dual nature instead of trying to suppress it. The fundamental trade-off is not between having technology and not having it, but between unregulated use and responsible management. States must find ways to take advantage of technology's benefits while limiting its misuse through targeted regulations, oversight and innovation that prioritise security and freedom. This balanced approach acknowledges that technology is neutral—its impact depends on how it is used and controlled.

Responsible governance is crucial for sustainable counter-terrorism. States should create clear legal frameworks that define the limits of surveillance, data collection and cyber operations, ensuring accountability through independent oversight. Incorporating democratic principles and human rights into counter-terrorism technologies helps maintain public trust, which is vital for long-term effectiveness. Investments in technological tools must be paired with investments in human intelligence, community interaction and social programmes that tackle the root causes of radicalisation. Technology alone cannot address deeply rooted social and political problems and the individual's bad motives or criminal intentions, as it is limited in detecting emotional intelligence.

International cooperation is also essential, as terrorism and cyber threats cross national borders. Multilateral agreements on intelligence sharing, cyber norms and technology transfer controls can harmonise global efforts while closing gaps that terrorists exploit. Public–private partnerships are particularly valuable in this realm. Technology companies, which control many of the platforms terrorists use, should work together with governments to develop privacy-conscious solutions that disrupt

extremist activity without limiting free expression. Societies must also invest in digital literacy, helping citizens recognise and reject extremist propaganda online. Counter-narratives should be credible, relevant to local communities, and culturally sensitive to lessen the appeal of extremist ideology.

Looking ahead requires careful planning. Artificial intelligence, quantum computing and autonomous systems will impact terrorism and counter-terrorism. Ethical guidelines, impact assessments and risk management frameworks should be established before these technologies are widely deployed. Without such preparation, states risk being caught off guard by the next technological advancement in extremist innovation.

Public trust and social resilience enhance counter-terrorism efforts. Communities that trust state institutions are more likely to cooperate with authorities, resist extremist recruitment and provide valuable intelligence. However, when counter-terrorism technologies are seen as intrusive or discriminatory, trust diminishes, creating a favourable environment for extremist narratives. Open communication between governments and civil society is vital. Being transparent about the purpose, scope and limitations of technological surveillance helps build legitimacy. Protecting civil rights and establishing accountability measures show that security does not come at the expense of democracy. States can shift technology from a contested tool to a shared defence by promoting inclusion, fairness and trust.

The struggle between technology, terror and the state is a defining aspect of modern security. Technology gives governments powerful tools to protect citizens, but it also provides terrorists with new means of violence and disruption. States have significant advantages in resources, expertise and legitimacy, while terrorists exploit anonymity, agility and innovation to counter these strengths. The main challenge is not achieving total victory, as this struggle is ongoing, but managing it responsibly. The fundamental trade-off is between unchecked use and guided application, where technology can serve security and freedom.

To navigate this complex landscape, states must pursue strategies that combine technological innovation with ethical governance, international cooperation and resilient societies. Only through such balanced approaches can states ensure that technology bolsters security while upholding the democratic values and freedoms that terrorists aim to undermine.

About the Author

Dr. Ntogwa N. Bundala, India-Africa Security Fellow, MP-IDSA

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

© Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) 2025

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses