Security Implications of Advancements in Neuroscience and Neurotechnology

V Krithika, Aayushi Sharma, Suryesh Kumar Namdeo

Ms. V Krithika is a Research Intern at the Centre for Society and Policy, Indian Institute of Science (IISc)

Ms. Aayushi Sharma is a Research Analyst at Manohar Parrikar Institute for Defence Studies and Analyses

Dr. Suryesh Kumar Namdeo is a Senior Research Analyst at the Indian Institute of Science (IISc)

Summary

This article examines the security implications of the advancements in neuroscience and neurotechnology in the context of civil-military convergence and relevance to the CBW regime. The article also looks at the various national and multilateral initiatives toward neurosecurity and outlines the way forward for India.

Introduction

For decades, strategic competition has been defined across five operational domains: land, sea, air, space, and cyberspace. Today, the sixth domain is emerging, one that does not lie beyond our borders but within ourselves.[1]

Advances in neurotechnology are increasingly positioning human cognition as the sixth domain of national security. Unlike the other domains in which states conduct military operations and compete for strategic advantage, cognition is the underlying substrate from which all other domains derive their strategic value. What is changing today is that the mind is no longer only the source of power; it is becoming the target of power. If the controller itself becomes the target, the security of every other domain is called into question.

The accelerating pace of innovation in neurotechnology is redefining the relationship between scientific progress and national security. Technologies developed to diagnose neurological disorders, restore lost function, and improve human health are now extending beyond the clinical abode into domains of strategic relevance.[2] Brain-computer interfaces, neuromodulation, cognitive enhancements, neuroimaging, neural decoding, and AI-enabled cognitive systems are no longer limited to medical applications. They are increasingly being developed for defence, intelligence, and national security.

Historical Underpinnings

The intersection of neuroscience and national security is not a novel phenomenon. As geopolitical tensions intensified during the Cold War, competition extended beyond

conventional military capabilities into intelligence, psychology, and human performance optimisation.[3] Military organisations and intelligence agencies became increasingly interested in understanding perception, memory, decision-making, learning, and behaviour. The focus gradually expanded from conventional military capabilities to the human brain itself, as questions about interrogation, soldier performance, and the influence of human behaviour gained strategic significance.[4]

One of the earliest documented initiatives was Project Bluebird, established by the Central Intelligence Agency (CIA) in 1950.[5] Initially developed to improve interrogation techniques, the program explored whether psychological methods, hypnosis, and pharmacological agents could alter memory and increase cooperation among prisoners. It marked one of the earliest efforts to investigate cognition as an intelligence tool. Operation Artichoke (1951) extended this line of research by investigating whether individuals could be conditioned, manipulated, or controlled for intelligence purposes.[6]

Collectively, Bluebird and Artichoke demonstrated an emerging strategic belief that the human mind could become an operational domain comparable to conventional military capabilities. These efforts culminated in 1953 with the launch of Project MK-ULTRA, the CIA's most extensive and controversial cognitive research programme. Spanning more than 149 subprojects, MK-ULTRA involved universities, hospitals, and private institutions, while also exposing profound ethical failures in state-sponsored cognitive research.[7] The project aimed to investigate a range of methods to influence cognition and behaviour in support of intelligence and interrogation objectives.[8] Although the programme failed to establish reliable methods of mind control, it demonstrated the extent to which governments were willing to treat cognition as a matter of national security.

These developments were compounded by the technological revolution in neuroscience and the advent of electroencephalography (EEG), followed by neuroimaging technologies such as CT, MRI, fMRI, PET, and MEG.[9] As a result of these advances, it became possible to observe cognition through biological foundations instead of sole reliance on behavioural inference, thus enabling systematic measurement and mapping of neurological activities. Brain-Computer Interfaces further established direct communication pathways between the brain and external devices.[10] Complementing these advances, neuromodulation technologies such as deep brain stimulation (DBS), transcranial magnetic stimulation (TMS), and transcranial direct current stimulation (tDCS) demonstrated that neural activity could not only be measured but also deliberately modulated. Although developed primarily for therapeutic purposes, these technologies have gradually attracted defence interest for their potential to enhance attention, learning, cognitive performance, fatigue resistance, and overall soldier effectiveness.[11]

Civilian-Military Convergence

The distinction between civilian and military dimensions of neuroscience is blurred even further, owing to the inherently dual-use nature of neurotechnology.[12] Innovations emerging from civilian laboratories, healthcare systems, and commercial enterprises are shaping future military capabilities and national security planning.[13]

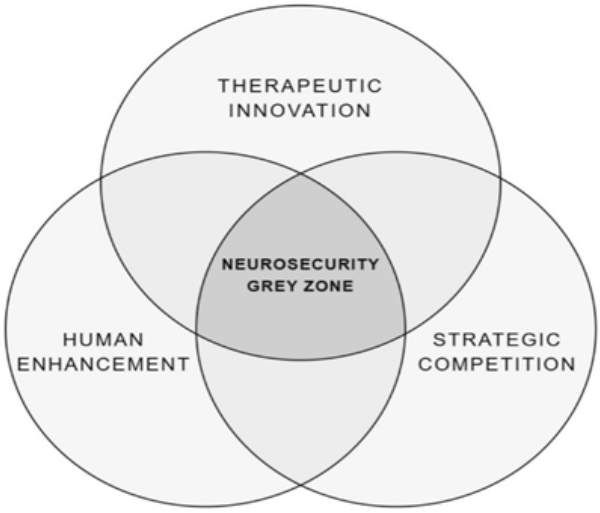

Figure 1.1 depicts the neurosecurity grey zone as the central intersection of therapeutic innovation, human enhancement, and strategic competition**.**

The "neurosecurity grey zone" depicts the intersection of civilian and military applications, as well as therapeutic innovation. Governing this grey zone would require policy frameworks that can manage the risks of dual-use neurotechnologies. Understanding this grey zone[14] is essential, as the principal challenge is not that neurotechnologies possess military utility; history suggests that transformative technologies routinely diffuse across civilian and defence sectors. The focus of neurosecurity thus points to safeguarding cognitive sovereignty as the human brain becomes both the object of innovation and a potential target of strategic competition.

This challenge is further complicated by the way neurotechnologies are developed and disseminated**.** Rather than moving sequentially between civilian and military domains, neurotechnology increasingly develops through a circular innovation cycle in which advances continuously flow between research, defence, and commercial sectors.[15]

Relevance to the CBW regime

With developments in neurotechnology, the avenues for application have shifted from restoring neurological functions to optimizing human performance. The same advances, however, also expanded the offensive dimensions of neurotechnology. In addition to human enhancement, growing attention was directed toward capabilities that could disrupt or manipulate an adversary's nervous system, giving rise to concerns over the development of neuroweapons.[16]

The delivery of neurological inhibitors has been examined through chemical and biological sources as well. Research into lethal chemicals with vast neurotoxic impacts has a long history, dating back centuries. Several nerve agents, such as Sarin, Tabun, Novichok, or VX, which are lethal even in small quantities, were considered for their potential neurotoxic implications.[17] These specific nerve agents inhibit acetylcholinesterase (AChE), which breaks down the neurotransmitter acetylcholine after a nerve signal. When AChE is inhibited, acetylcholine accumulates in the body, causing physiological and neurological symptoms manifesting as muscle fasciculations, seizures, or respiratory failure.[18] In the case of chemical weapons, several Central Nervous System (CNS)- acting chemicals have also been identified, which target the brain and the spinal cord, leading to physiological, neurological, and psychological impacts.

Along with chemical sources, naturally derived toxins or biotoxins also became significant sources of weaponisation for neurological impacts. Botulinum toxin became central to these discussions because of its ability to directly interfere with neural transmission, while anthrax demonstrated that biological agents need not specifically target the nervous system to produce severe neurological consequences.[19]

This indicates that developments in neuroscience and neurotechnology intersect significantly with those in the chemical and biological security domain. The Chemical

Weapons Convention (CWC) and the Biological Weapons Convention (BWC) have exerted broad legal influence on emerging challenges through their general-purpose criterion prohibitions. However, the implementation institutions, or their lack thereof in the case of the BWC, struggle with converging risks, hybrid agents, and their rapidly developing production methods, which also blur the existing boundaries.

This means that Central Nervous System (CNS)-acting agents, mid-spectrum agents, and bioregulators are covered in principle by the general-purpose criterion of the BWC and the CWC; gaps in practical governance still exist. The chemical weapons disarmament regime has paid certain attention to the CNS-acting agents, leading up to the landmark declaration on the aerosolised delivery of CNS- acting chemicals such as opioid fentanyl and its analogues. The declaration differentiated the issue of CNS-acting agents from that of the Riot Control Agents (RCAs).[20] While this recognition is substantial, the CWC does not comprehensively cover the CNS-acting agents in the Schedules, aside from BZ (3-quinuclidinyl benzilate) and its precursors[21], leading to regulatory gaps and potential oversight. The operational and implementation challenges within the BWC also add to the gaps in the regulation and governance of the biotoxins with neurological effects.

Existing National and Multilateral Approaches

While the challenges to the international legal frameworks persist, the convergence of neurosecurity with other emerging technological capabilities will also have direct implications for the national security landscape. This is reflected in the efforts to assess the security significance of neurotechnology that have emerged through a multitude of key institutions and policy frameworks across several countries and multilateral institutions. Conversely, initiatives such as the International Brain Initiative stand as a civil society consortium bringing together researchers and scientists working toward civilian or therapeutic uses of neuroscience.[22]

Table 1: Key institutions and policy frameworks on neurosecurity across countries

	National Approach	**Key Institutions/Programmes**	**National Frameworks**
US	Dual-use innovation, Decentralised, multi-agency federal model	NIH - BRAIN Initiative (2013) DARPA - Restoring Active Memory (RAM)[23] (2014) DARPA - Neural Engineering System Design (NESD) (2016)[24] IARPA - MICrONS Program 2016)[25] DARPA - Next-Generation Nonsurgical Neurotechnology (N3) (2019)[26] Neuralink, Synchron: private sectors	NIH-BRAIN 2025 2014) NIH - BRAIN Initiative 2.0 (2019) DoD - National Defense Strategy (2022) White House - Executive Order 14110 (2023) BIS - Export Administration Regulations (EAR)
China	Civil-Military Fusion, Centralised, state-led	MOST- China Brain Project (2016) CAS - Brain Science and Brain-Inspired Intelligence Program (2015) CIBR - Brain Research Program (2018)	State Council-Military-Civil Fusion Strategy (2015) State Council - New Generation Artificial Intelligence Development Plan 2017)

	National Approach	Key Institutions/Programmes	National Frameworks
EU	Responsible innovation, Multi-level Governance	European Commission - Human Brain Project (2013) European Commission - EBRAINS (2020) European Commission - Horizon Europe (2021)	European Commission - Human Brain Project Ethics Framework (2013) European Commission - EBRAINS Ethics & Data Governance Framework (2020) European Union - GDPR (2016/2018) European Defence Fund - Defence Research Programme (2021)
Japan	Society 5.0, Government-led, cross-ministerial	MEXT - Brain/MINDS Project (2014) AMED - Brain/MINDS Beyond (2018) ATR - Brain Information Communication Research (ongoing) ATLA - Advanced Technology Research Programme (ongoing)	Cabinet Office - Society 5.0 (2016) Cabinet Office - Integrated Innovation Strategy (2018) MOD/ATLA - Defense Technology Strategy (2022)
South Korea	Government-led, multi-agency Centralized, ministry-led	MSIT - Korea Brain Initiative (2016) KBRI - Korea Brain Research Institute (2011) KIST - Brain Science Research (ongoing) ADD - Defense AI & Human–Machine Teaming Research (ongoing)	MSIT- Fourth Basic Plan for Brain Research Promotion (2023-2027) Government of Korea-Digital Strategy (2022) Ministry of National Defense- Defense Innovation 4.0 (2023)
Australia	Translational Innovation, Decentralized, research-led	University of Melbourne -Synchron BCI Research Synchron - Stentrode BCI (2012) Defence Science and Technology Group (DSTG) - Human Performance Research Australian National University (ANU) (ongoing)	Department of Defence - Defence Science and Technology Strategy 2030 Department of Defence - Defence Innovation, Science and Technology Strategy (2024)

Table 2: Key initiatives by multilateral organisations

Multilateral Organisations	Key Projects and Initiatives
North Atlantic Treaty Organisation (NATO)	Emerging & Disruptive Technologies (EDT) Strategy (2021) NATO Innovation Fund (2022) NATO DIANA (2023) NATO STO – Human Factors & Medicine (HFM) Panel (1998–present)
United Nations Educational, Scientific and Cultural Organization (UNESCO)	Recommendation on the Ethics of Neurotechnology (2025)
Organisation for Economic Co-operation and Development (OECD)	Recommendation on Responsible Innovation in Neurotechnology (2019)

India's National Policy Pathways

With the regulatory ambiguities introduced by emerging technologies, the potential for neurobiological misuse also increases multifold. The question of neurosecurity involves diverse aspects of chemical security, biosecurity, cybergovernance, AI safety, disarmament, human rights, and scientific oversight; hence, national policy approaches to address this emerging domain must also account for these dimensions. Certain steps could thus contribute toward an integrated national approach to address risks associated with neurosecurity.

1. **Anticipatory governance** - Anticipatory governance mechanisms could include systematic science and technology reviews, revised export controls, data security protocols, institutional ethical reviews of research in line with global frameworks[27], and multi-layered stakeholder engagement. This could be institutionalised by establishing an advisory board supported by a secretariat at the Office of the Principal Scientific Advisor to the Government of India.

2. **Embed Security by Design[28] and Privacy by Design**: Cybersecurity, privacy, and resilience should be embedded into neurotechnologies from the earliest stages of research and development, ensuring that neural systems are secure before deployment rather than protected afterwards. Here, agencies including the Ministry of Electronics and Information Technology (MeitY) and the Central Drugs Standard Control Organisation (CDSCO) should incentivise and regulate the development and deployment of such systems in the country.

3. **Strengthen Indigenous Neurotechnology and Neurosecurity Capabilities**: Greater investment in domestic research, innovation, and manufacturing will reduce dependence on foreign neurotechnologies while strengthening India's strategic and technological resilience. Here, a dedicated DRDO Young Scientists Laboratory could be established in partnership with academia and industry. Further, the Research, Development and Innovation (RDI) fund

under ANRF could be leveraged for supporting start-ups that are indigenously developing these capabilities. Lastly, joint calls for proposals with strategic partner countries could be launched to co-develop certain niche technologies, where the country lags.

4. **Develop rules and norms for protecting neural data:** Specific rules under the Digital Personal Data Protection Act, 2023 should be developed alongside AI Safety norms for protecting neural data from theft, misuse, manipulation, etc. Here, a Centre of Excellence should be established to support these efforts by bringing technical and policy expertise together to analyse global practices, sovereignty and security requirements, industrial benchmarking and technical gaps.

5. **Lead Global Discourse:** India has a strategic opportunity to lead and shape global discourse in strengthening safe, secure and responsible use of neuroscience and neurotechnology. It should convene international experts for focused discussions during the G20, BRICS, SCO and Quad meetings, and actively shape the deliberations at UNESCO. Further, it should leverage the Chief Science Advisors Roundtable (CSAR) mechanism, which it helped establish, to develop international norms for safe and secure development of neurotechnology.

Overall, the emerging challenges also provide India with an opportunity to develop indigenous capabilities and become a leader in shaping international norms, rules, and regulations for the safe and secure development of neurotechnology.

Views expressed are of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or of the Government of India.

Endnotes:

1 Pierrick Devidal, "Cognitive warfare": why the human brain should not become a battlefield, Humanitarian Law & Policy Blog, International Committee of the Red Cross (ICRC), 5 February 2026.

2 Marcello Ienca, Fabrice Jotterand and Bernice S. Elger, "From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?", Neuron, 17 January 2018.

3 The New Yorker, "Secrets of Edgewood", The New Yorker, 21 December 2012.

4 Claes Tängh Wrangel, "The biopolitics of algorithmic governmentality: How the US military imagines war in the age of neurobiology and artificial intelligence", Security Dialogue, 9 May 2024.

5 Central Intelligence Agency (CIA), "Project Bluebird", Central Intelligence Agency (CIA), 5 April 1950

6 Central Intelligence Agency (CIA), "Background Literature on Behavior Control and Drugs of Interest to Project ARTICHOKE/ BLUEBIRD", Central Intelligence Agency, Declassified 1 May 2002

7 Encyclopaedia Britannica, "MK-ULTRA", Encyclopaedia Britannica

8 Lukas J Meier, "Mind Control: Past and Future", Carr Center for Human Rights Poliyc, Harvard Kennedy School, 13 January 2025

9 Marcus E. Raichle, "A Brief History of Human Brain Mapping", Trends in Neurosciences, February 2009

10 Robbin A. Miranda, William D. Casebeer, Amy M. Hein, Jack W. Judy, Eric P. Krotkov, Tracy L. Laabs, Justin E. Manzo, Kent G. Pankratz, Gill A. Pratt, Justin C. Sanchez, Douglas J. Weber, Tracey L. Wheeler and Geoffrey S. F. Ling, "DARPA-funded efforts in the development of novel brain–computer

interface technologies", Journal of Neuroscience Methods, 15 April 2015

[11] Federico Mantellassi and Edward Madziwa, "Neurotechnology in the Military Domain: A Primer", United Nations Institute for Disarmament Research (UNIDIR), 4 November 2025

[12] Alison Howell, "Neuroscience and War: Human Enhancement, Soldier Rehabilitation, and the Ethical Limits of Dual-use Frameworks", Millennium: Journal of International Studies, January 2017

[13] Marcello Ienca, Fabrice Jotterand and Bernice S. Elger, "From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?", Neuron, 18 December 2017

[14] Hailee Carter, "Cognitive Sovereignty and the Neurosecurity Governance Gap: Evidence from Singapore", arXiv, 15 December 2025

[15] Marcello Ienca, Fabrice Jotterand and Bernice S. Elger, "From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?", Neuron, 18 December 2017

[16] Douglas J. Lanska, "Neurologic Disorders Related to Biological Warfare Agents and Toxins", MedLink Neurology

[17] Vladimír Pitschmann and Zdenìk Hon, "Drugs as Chemical Weapons: Past and Perspectives", Toxics, 4 January, 2023

[18] Vassiliki Aroniadou-Anderjaska, James P. Apland, Taiza H. Figueiredo, Marcio De Araujo Furtado and Maria F. Braga, "Acetylcholinesterase inhibitors (nerve agents) as weapons of mass destruction: History, mechanisms of action, and medical countermeasures", Neuropharmacology, 15 December 2020.

[19] Ilkhchoui Yashar, Ghaly Ramsis F., Knezevic N. Nick, and Candido Kenneth D., "Central Nervous System Toxicity After Botulinum Neurotoxin Injection", Anesthesiology and Pain Medicine, 1 July 2013

[20] Organisation for the Prohibition of Chemical Weapons (OPCW), "Understanding Regarding the Aerosolised Use of Central Nervous System-Acting Chemicals for Law Enforcement Purposes", Decision C-26/ DEC.10, 1 December 2021

[21] Organisation for the Prohibition of Chemical Weapons (OPCW), "Schedule 2", Annex on Chemicals, Chemical Weapons Convention.

[22] International Brain Initiative, "International Brain Initiative: An Innovative Framework for Coordinated Global Brain Research Efforts", Neuron, 22 January 2020

[23] Defense Advanced Research Projects Agency (DARPA), "Restoring Active Memory (RAM)", Biological Technologies Office, U.S. Department of Defense

[24] Defense Advanced Research Projects Agency (DARPA), "Neural Engineering System Design (NESD)", Biological Technologies Office, U.S. Department of Defense.

[25] Intelligence Advanced Research Projects Activity (IARPA), "Machine Intelligence from Cortical Networks (MICrONS)", U.S. Office of the Director of National Intelligence, 8 January 2015

[26] Defense Advanced Research Projects Agency (DARPA), "Next-Generation Nonsurgical Neurotechnology (N^3)", Biological Technologies Office, U.S. Department of Defense, 16 March 2018

[27] UNESCO, "Ethics of neurotechnology: UNESCO adopts the first global standard in the cutting-edge technology", Press Release, 5 November 2025

[28] Tamara Denning, Yoky Matsuoka, and Tadayoshi Kohno, "Neurosecurity: Security and Privacy for Neural Devices", Neurosurgical Focus, July 2009