Neural Frontiers: Repositioning India's Cybersecurity Diplomacy in the Neurotechnology Era

Kritika

Introduction

The human brain has long been a target of warfare. From initial psychological processes to the contemporary influence campaigns, adversaries have recognised the that controlling of cognitive environment yields decisive strategic advantage. The contemporary period is defined by the emergence of neurotechnology, which implies the creation of direct interface between digital systems and human brain as operationally possible.

Brain Computer Interfaces (BCIs) have gone beyond the scope of researches into the practical implementation of devices aimed at understanding neural processes and protecting the human brain from possible damages. They are utilised not only to understand neural activities better, but also as means of protecting neural information from malevolent hackers that can jeopardise personal well-being and national security. In addition to that, BCIs represent one of the elements of contemporary military and business practice. Furthermore, they are used for intelligence gathering purposes by governments. Unfortunately, the approaches developed by India for securing its networks and computer infrastructure are rather limited in addressing the challenge in the context of neurotechnologies.

Thus, the country lacks any measures that could address the problem on the neural level while maintaining the focus primarily on the protection of network infrastructure. The paper contends that neuro-cybersecurity, which is a distinctive and pressing sub-field of cyber diplomacy, suffers from certain structural vulnerabilities, which means that an appropriate strategy based on the three-track approach involving norm entrepreneurship, bilateralism, and institution-building, among others, can help India gain a security advantage and position as a global leader.

The Neurotechnology and Cybersecurity Nexus

Neuro-Cybersecurity is defined as the safeguarding of neural information, BCI, and cognition from cyberattacks. There are three distinct areas of threats that constitute the concept of neuro-cybersecurity. First, is neural data privacy. BCIs and consumer neurotech gadgets create Electroencephalographic (EEG) information, which discloses details about cognitive functions, emotional responses, and even classified information processed by defence and intelligence experts.[1] The second, is cognitive hacking, where an adversary can manipulate BCIs and use them as a backdoor to access sensory information, disable motor information, or cause cognitive disruption in military personnel.[2] Third is an adversarial neurotechnology, where weapons systems are developed to inhibit brain function through the choice of either

electromagnetic or ultrasonic interference.[3] According to press reports, both China and Russia have ongoing programs in this regard.

The Diplomatic Imperative

Tallinn Manual 2.0, the most authoritative attempt to apply international law to cyber operations makes no mention of neural data or BCI systems.[4] Furthermore, the Open-ended Working Group (OEWG) and the United Nations Group of Governmental Experts (UNGGE) have not considered the aspect of neural technology, creating doubts about attribution, accountability, and proportionality in relation to any attacks by using neuro-technology on military forces.[5] For India, a country that is developing its ecosystem of research involving BCIs beyond laboratories, this poses a major threat since it is a country that is highly vulnerable to the advancements made by its opponents with regard to neurotechnology.

India's Cybersecurity Diplomatic Architecture

The Indian government has been participating actively in the UNGGE and OEWG processes, and it has subscribed to 11voluntary norms of responsible state behaviour in cyberspace.[6] The Indian government's National Cyber Security Policy, 2013 continues to be the basis for cyber governance in India, and the Defence Cyber Agency, which was created in 2019, offers military cyber capabilities. Nevertheless, there is no focus on neural data issues in the policy documents. The Defence Research and Development Organisation is carrying out research in neuroscience at present, but there is no systematic connection between its findings and the diplomatic position of India regarding cybersecurity matters.

Challenges Confronting India

At the international level, there is no definition of neuro-cybersecurity. The dual use of neurotechnology poses a challenge to adopting an approach that involves treaties. India, like all other nations, lacks the legal mechanisms to bring offenders to book for carrying out cyberattacks through neurotechnology.[7] Open norm-building offers opportunities and challenges for India. In the military-civil fusion strategy followed by China, neuroscience plays an explicit role in defence research, as can be observed from the People's Liberation Army's publications on warfare in the cognitive realm.[8] India's Ministry of External Affairs lacks diplomats who are well versed in neuro-cybersecurity, while the Sushma Swaraj Institute of Foreign Service does not offer courses on neurotechnology governance.

Emerging International Precedents on Neural Data Governance

A number of jurisdictions have already started building the initial framework of neuro-rights law, providing both lessons from bad practice and models to follow for India. First of all, Chile, in 2021, introduced amendments to its Political Constitution, becoming the first state in the world to introduce neuro-rights on a constitutional level and protect citizens' mental integrity by forbidding unauthorised modifications or manipulations of their brain activity.[9] This development was highly praised by jurists,

who considered it the dawn of a new chapter in the book of human rights legislation. Another example of how to incorporate the notion of neuro-rights into national legislation is found in the European Union Artificial Intelligence (AI) Act (2024).[10] Although this act regulates the use of AI, some parts of it are also relevant for neural biometric devices.

The Neuro-rights Foundation at Columbia University has been able to achieve legislative success by lobbying several states in the United States. For instance, Colorado was the first to extend comprehensive privacy rights to neural data under HB 24-1058 (2024).[11] Following Colorado, the state of Minnesota passed the Consumer Data Privacy Act (HF 4757, 2024), where neural data is categorised as one of the types of sensitive personal information that merits stronger legal protection. The most important milestone till date is the adoption of the United Nations Educational, Scientific and Cultural Organization Recommendation on the Ethics of Neurotechnology in 2025, which recognises cognitive liberty, mental privacy, and psychological continuity as essential human rights that deserve legislative recognition in the digital era.[12] It is clear from the above facts that the window for neuro-cybersecurity governance is being filled most times, without India being at the table. This marks a significant strategic weakness for India given its democratic credentials and scientific competence.

A Three-Track Strategic Framework for India

India being the world's largest democracy, the voice of the Global South, and technologically equipped for multilateral commitment sets the scene for norm entrepreneurship in neuro-cybersecurity. India must do something in order to make neuro-cybersecurity an official issue in the UNGGE and OEWG. The Quadrilateral Security Dialogue alliance comes the closest when it comes to neuro-cybersecurity cooperation as all its members are aware of China's capabilities in cognitive warfare, actively conducting BCI research programs, and willing to cooperate on the topic of controlling emerging technologies. The passage of the Neural Data Protection Framework will not only ensure better protection for the citizens of India[13] but also bolster its standing as a norm entrepreneur on the international stage.

Conclusion

Neuroscience and cyberspace are no longer just two worlds that are yet to merge but two technologies whose fusion is already a practical reality. The diplomatic structure established by India to deal with the network-centric threats in the last decade falls short in addressing this emerging phenomenon. The policy scope of influence regarding the international norming process in this regard is wide and contracting. India possesses the credentials of democracy, scientific acumen, and diplomatic credibility to assume the norm entrepreneur role in this realm. The debate is no longer about whether India has the potential to become a frontrunner, but rather whether the country will take action on its own initiative prior to other states to establish the structure of neuro-cybersecurity governance. Whichever state establishes the rules of

neuro-cybersecurity governance today will have the advantage in tomorrow's cognitive warfare.

References

[1] Sergio López Bernal, Alberto Huertas Celdrán, Gregorio Martínez Pérez, Michael Taynnan Barros, and Sasitharan Balasubramaniam, "Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges", *ACM computing surveys (CSUR)* 54, no. 1: pp 1-35, 02 Jan 2021, accessed 20 Apr 2026, https://dl.acm.org/doi/10.1145/3427376

[2] Øyvind Voie and Susanne Glenna, "Human Enhancement Technologies and the Possible Dual Use in Cognitive Warfare", *NATO Science and Technology Organization*, 2024, accessed 21 Apr 2026, https://www.sto.nato.int/document/human-enhancement-technologies-and-the-possible-dual-use-in-cognitive-warfare/

[3] Elsa B Kania and Wilson Vorndick, "Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare'", *Defense one* 14, 14 Aug 2019, accessed 22 Apr 2026, https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/

[4] Ashutosh Pandey, "Application of International Humanitarian Law in Changing Dimensions of Armed Conflict vis-à-vis Cyber Warfare", *Unity Journal* 6, no. 1: 284-296, 25 Feb 2025, accessed 23 Apr 2026, https://doi.org/10.3126/unityj.v6i1.75698

[5] United Nations, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", A/76/135, 14 Jul 2021, accessed 24 Apr 2026, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[6] United Nations Office for Disarmament Affairs, "Fact Sheet: Responsible State Behaviour in Cyberspace", Mar 2022, accessed 24 Apr 2026, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[7] Kritika, "Ethical and legal dimensions of integrating neurotechnology with cybersecurity, a critical reflection for information and communication technology (ICT) policy and practice", *International Cybersecurity Law Review* (2026): 1-61, accessed 24 Apr 2026, https://link.springer.com/article/10.1365/s43439-026-00168-6

[8] Larry M Wortzel, "Chinese Expectations for Biotechnology And Cognitive Enhancement in Future Warfare', *Modern War Institute at West Point*, 2022, accessed 21 Apr 2026, https://mwi.westpoint.edu/wp-content/uploads/2022/10/2022-10-05-MWI_Chinese_Biotechnology_Wortzel.pdf

[9] República de Chile, "Ley No. 21.383: Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas", *Biblioteca del Congreso Nacional*, Oct 2021, accessed 24 Apr 2026, https://www.bcn.cl/leychile/navegar?idNorma=1166983

[10] European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", *Official Journal of the European Union*, L 2024/1689, 12 Jul 2024, Articles 6–7, accessed 24 Apr 2026, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[11] Colorado General Assembly, "HB 24-1058: Concerning Protecting the Privacy of Individuals' Biological Data, and, in Connection Therewith, Protecting the Privacy of Neural Data and Expanding the Scope of the Colorado Privacy Act Accordingly", signed 17 Apr 2024, accessed 22 Apr 2026, https://leg.colorado.gov/bills/hb24-1058

[12] UNESCO, "Recommendation on the Ethics of Neurotechnology," adopted at the *43rd Session of the General Conference*, Nov 2025, accessed 23 Apr 2026, https://www.unesco.org/en/ethics-neurotech/recommendation

[13] Kritika, "Ethical and Policy Considerations in Neuro-Integrated Security", In *Neuroscience Meets Cybersecurity: Applying Brain Science to Enhance Digital Protection*, (Berkeley, CA: Apress, 2026), pp 311-354.

Ms Kritika is an experienced interdisciplinary researcher specialising in the bridging of human, technical, and organisational perspectives of digital risk. Her work spans over the disciplines of cybersecurity, neuro-cybersecurity, human centric psychology and cyber diplomacy.

Article uploaded on 07-05-2026