Commercial Neurotech and the Risks of Cognitive Warfare

Łukasz Kamieński[1]

[1] Department of Interantional and Political Studies, Jagiellonian University in Krakow, Poland; 2025-2026 Fulbright Visiting Scholar, University of Pennsylvania

Synopsis

Commercial neurotechnologies, particularly wearable brain-monitoring devices and non-invasive brain-computer interfaces, are rapidly moving from therapeutic contexts into everyday consumer markets. This transition will generate large volumes of highly sensitive neurodata that can reveal users' cognitive states in near-real time, including attention, fatigue, stress, and affective responses. This paper investigates how such neurodata might become a strategic dual-use asset. Building on the concept of cognitive warfare and scholarship on data flows and privacy, it develops a risk-pathway account of how brain data can be trafficked across jurisdictions and then operationalized for malicious, micro-targeted cognitive influence and behavior manipulation.

Background

Consumer neurotechnology is expanding beyond therapeutic applications into lifestyle, wellness, entertainment, and productivity. Big Tech companies, including Meta, Snap, Microsoft, Google, Merge Labs, and Apple, as well as numerous start-ups such as Alljoined, Alter Ego, Conduit, and Forest Neurotech, have increasingly invested in brain wearables to advance their adoption for everyday use [1, 2]. Devices that employ brain monitoring (e.g., EEG- and ultrasound-based wearables) aim to detect cognitive states, such as attention/alertness, workload, stress, and mood proxies. These products will increasingly be embedded in everyday devices, such as headbands, earbuds, headphones, and sleep aids, making neurodata collection more ambient and continuous while also making it more difficult for users to meaningfully assess [3].

Neuroethical discussions typically focus on mental privacy, autonomy, and liberty [4], yet an important geostrategic security dimension remains overlooked. Meanwhile, neurodata can be valuable not only for personalized neuromarketing within the current "attention economy" [5] but also for hostile influence operations, turning commercial neurotech into a new platform for what NATO and security experts have identified as "cognitive warfare" (CogWar) [6, 7, 8]. This concept describes an unconventional form of conflict in which adversaries target the human mind by shaping individuals' and groups' perceptions, beliefs, and decision-making [8, 9]. The aim is not to change what people think but rather *how* they think. The CogWar threat is not hypothetical, as authoritarian regimes, including China and Russia, have conducted and refined malicious influence campaigns against civilian populations in democratic societies, aimed at creating confusion, sowing distrust, exacerbating divisions, undermining institutions, and shaping perceptions in line with their narratives [10, 11].

The paper investigates how consumer-grade neurotechnologies and the neurodata they collect might facilitate more sophisticated forms of CogWar.

Methods

To assess the risks posed by the rapid expansion of commercial neurotech, the paper employs a qualitative, multidisciplinary approach that draws on neurotechnology research and neuroethics on the one hand, and security studies on the other. The analysis combines three conceptual elements:

1. Building on NATO's framing and relevant scholarship, the paper refines the concept of *cognitive warfare* by foregrounding one of its distinguishing features: the enabling potential of emerging disruptive technologies for malicious operations, as exemplified by neurotechnologies.
2. Drawing on the concept of *data trafficking* [12], the paper highlights how neurodata collected by commercial neurodevices (particularly those manufactured abroad) can flow across platforms, cloud services, and jurisdictions in ways that remain opaque to users. Such transfers may enable third-party access without users' awareness or consent and may occur beyond the reach of effective state oversight. An additional concern is the potential acquisition of a domestic company by a foreign entity, which could result in the cross-border transfer of neurodata to a foreign jurisdiction.
3. It expands the concept of *neurosecurity*, originally defined in the context of medical neurotechnologies as "the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will" [13]. In the domain of national security, the paper redefines *neurosecurity* as the protection of the confidentiality and integrity of neurodevices and neurodata to safeguard national cognitive autonomy.

Results

The analysis yields three main findings:

First, neurodata collected by commercial neurotech constitutes a critical dual-use strategic asset that can be weaponized for cognitive influence operations by providing granular indicators of users' attentional states, fatigue, stress, and affective reactivity.

Second, data mined by neurodevices can be aggregated with other personal and biometric information (digital fingerprints, online behavior, and life patterns) for AI-driven psychological profiling and sentiment analysis. This integrated data enables real-time content adaptation, supporting hyper-personalized targeting in which timing and framing can be tuned to moments of heightened individual vulnerability (e.g., low vigilance, exhaustion, high arousal, elevated stress).

Third, these dynamics suggest that as the potential disruptive role of commercial neurotechnologies in malign CogWar operations grows, their regulation, particularly of the data they collect, store, and transmit, is an urgent governance priority that existing frameworks are ill-equipped to address.

Discussion

Current policy debates, exemplified by scrutiny of TikTok, focus primarily on data access and privacy violations. This framing, while valid, is insufficient. The more consequential risk is how biometric data, particularly those that capture cognitive and affective states, can be utilized for cognitive manipulation rather than merely harvested.

What distinguishes neurodata from conventional behavioral traces is its temporal granularity. Rather than inferring psychological states retrospectively from digital footprints, adversarial actors could exploit real-time windows of mental susceptibility by dynamically adjusting communication modality, content selection, emotional framing, and timing. This would shift influence operations from demographic targeting to individualized, moment-sensitive manipulation.

Regulatory asymmetries intensify these concerns. In particular, as Chinese neurodevices enter the U.S. market with weak data governance, a structural vulnerability emerges. For example, the Chinese company Entertech manufactures the Flowtime headset, a biosensing neurofeedback device that is increasingly popular in the United States and Europe for meditation [14, 15]. If

neurodata collected worldwide are stored in China, then under the civil-military fusion doctrine, they could be made available to the government as deemed necessary.

In sum, neurodata-enabled microtargeting would represent a significant shift in the character of CogWar, making the protection of the cognitive domain not merely an ethical or legal concern but a strategic imperative.

References

1. Livingston, I., et al. (2025). Sam Altman Challenges Elon Musk with Plans for Neuralink Rival. Financial Times. https://www.ft.com/content/04484164-724e-4fc2-92a2-e2c13ea639bd [Accessed January 7, 2025].
2. Toews, R. (2025). The Next Frontier for AI Is the Human Brain. Forbes. https://www.forbes.com/sites/robtoews/2025/12/07/the-next-frontier-for-ai-is-the-human-brain [Accessed January 7, 2026].
3. Estes, A. C. (2025). Headphones That Scan Your Brainwaves and Keep You Focused? It's Not Science Fiction. Vox. https://www.vox.com/science/422610/oura-ring-neurable-apple-airpods-brain-health [Accessed January 7, 2025].
4. Farahany, N. A. (2023). The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology. New York, NY: St. Martin's Press.
5. Celis Bueno, C. (2017). The Attention Economy: Labour, Time and Power in Cognitive Capitalism. London: Rowman & Littlefield International.
6. Claverie, B., Prébot, B., Buchler, N., and du Cluzel, F. (eds.) (2022). Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office.
7. Hoffman, F. (2025). Assessing "Cognitive Warfare". Small Wars Journal. https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/ [Accessed January 7, 2025].
8. NATO ACT. (2023). Cognitive Warfare: Strengthening and Defending the Mind. NATO's Strategic Warfare Development Command, Allied Command Transformation. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ [Accessed January 7, 2025].
9. Blatny, J. M., and Søndergaard, S. (2025). Cognitive Warfare. Office of the Chief Scientist, Science and Technology Organization, North Atlantic Treaty Organization. https://www.sto.nato.int/document/cognitive-warfare/ [Accessed January 7, 2025].
10. Desclaux, G., and Struye de Swielande, T. (2022). "China and Cognitive Warfare: Why Is the West Losing?," in Cognitive Warfare: The Future of Cognitive Dominance, eds. B. Claverie, B. Prébot, N. Buchler, and F. du Cluzel (NATO Collaboration Support Office), 2-1–2-8. https://hal.science/hal-03635889 [Accessed December 29, 2025].
11. Bugayova, N., and Stepanenko, K. (2025). A Primer on Russian Cognitive Warfare. Institute for the Study of War. https://understandingwar.org/sites/default/files/ISW%20CW%20Russian%20Cognitive%20Warfare%2C%20June%2030%2C%202025%20PDF%20FINAL_0.pdf [Accessed December 29, 2025].
12. Kokas, A. (2023). Trafficking Data: How China Is Winning the Battle for Digital Sovereignty. Oxford: Oxford University Press.
13. Denning, T., et al. (2009). Neurosecurity: Security and Privacy for Neural Devices. *Neurosurg. Focus* 27:E7. doi: 10.3171/2009.4.FOCUS0985
14. Flowtime. (n.d.). Flowtime: Biosensing Meditation Headband. https://www.meetflowtime.com/ [Accessed December 29, 2025].
15. Rickli, J.-M., and Ienca, M. (2021). "The Security and Military Implications of Neurotechnology and Artificial Intelligence," in Clinical Neurotechnology Meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications, eds. O. Friedrich et al. (Cham: Springer International Publishing), 197–214. doi: 10.1007/978-3-030-64590-8_15.