Cyberbiosecurity for Brain-Computer-Interfaces

1 APRIL 2026

Alisa Grunert



The convergence of biological sciences and digital infrastructure has necessitated the emergence of cyberbiosecurity, a discipline dedicated to understanding and mitigating vulnerabilities at the intersection of life sciences and computational systems. As technological advancements facilitate direct communication between the human nervous system and external devices, the relevance of this field has expanded beyond the laboratory into the realm of human cognition. These developments go naturally hand in hand with certain risks. Neurotechnology devices like BCIs can get hacked – to physically do harm or cause lethality and for the exploitation or extortion

of individuals, including military staff (DeFranco et al 2019: 57). With BCIs having entered the military and the commercial sector, they will profoundly transform warfare, adding another layer to vulnerable "infrastructure" with neurodata being involved.

Why is cyberbiosecurity relevant for emerging cyber-bio threats in the context of Brain-Computer-Interfaces (BCIs)? Its relevance stems from the fact that BCIs represent a unique cyber-physical-biological nexus where digital vulnerabilities can translate directly into neurological harms, the loss of cognitive freedom, and the creation of novel categories of kinetic and information warfare.

Cyberbiosecurity is defined as the effort to understand vulnerabilities to unwanted surveillance, intrusions, and malicious activities occurring at the interfaces of life and medical sciences, cyber-physical systems, and infrastructure (Murch et al. 2018). While traditional biosecurity focuses on the physical protection of biological agents and laboratories, cyberbiosecurity addresses threats originating in the digital domain, such as state-sponsored espionage, ransomware, and the exploitation of software vulnerabilities in biomanufacturing or diagnostic equipment (Lekatis 2026). In the context of BCIs, these threats are amplified as the *target* shifts from external biological data to the internal processes of the human brain.

Vulnerability of the Bio-Cyber-Sphere

The *bio-cyber-sphere* encompasses the networked hardware, data, and biological entities that comprise modern life science and neurotechnology. BCIs, such as the Neuralink system, are designed to modulate selective brain networks and functions, creating a direct conduit for data exchange between the brain and digital interfaces (DeFranco et al. 2019: 57). This connectivity introduces several critical vulnerabilities that can be categorized by the phase of BCI application and the nature of the attack vector.

According to Alohaly (2024), BCIs are susceptible to several distinct forms of cyber-attack:

Brain Tapping: During the signal acquisition phase, attackers can intercept signals transmitted from the brain. This compromises confidentiality by allowing the involuntary inference of highly sensitive information, including emotions, preferences, and religious or political beliefs. *Misleading Stimuli Attacks*: These attacks manipulate the integrity of the generated signal, leading to biased outcomes. Crucially, misleading stimuli can be used during the feedback phase to control an individual's mind or compel them to engage in actions contrary to their will. This is particularly dangerous when BCIs are used to control vehicles or weaponry. *Adversarial Attacks*: These target the machine learning components of BCIs. By manipulating training data, an attacker can skew results, such as biasing "brain fingerprinting" used in lie detection (Alohaly 2024).

The vulnerabilities are not limited to the BCI device itself but extend to the broader digital infrastructure. Life science laboratories and BCI developers possess vulnerabilities associated with networked hardware and facility systems (Reed & Dunaway, 2019: 13). Exploitation of these systems can jeopardize research data integrity, intellectual property, and even the physical safety of occupants.

Furthermore, the data generated by BCIs, neurodata, presents a *special* category of risk. Genomic neurodata, if accessed or manipulated, could potentially damage the brain's DNA or might target an individual's genetic vulnerability via precision agents (DeFranco et al. 2019: 57). BCIs function through a translation of brain activity into control signals. These signals arrive in respective devices and further provide a sensory feedback to stimulate the brain (Alohaly 2024). This highlights a fundamental cyber-biosecurity concern: the protection of the digital blueprints and neural data that define biological identity and function.

Legal and Ethical Implications

The integration of human intelligence with neuromorphic computing capabilities (H/nB) creates profound legal and ethical challenges that traditional frameworks are ill-equipped to handle. The transition from a human actor to a human/BCI merger transforms the individual into a potential weapon of war, capable of *cerebral force* that could preempt offensive measures by seeing and anticipating threats (Sharp 2020: 319, 337). There are countries with special programs on neuroenhancement and dual-use neurodevices, but they are only partly amenable or accessible to international inspection and surveillance (DeFranco et al. 2019: 58).

The ability to access and control human cognition, emotion, and behavior via BCIs incurs risks that demand stringent cyberbiosecurity solutions (DeFranco et al. 2019: 57). The potential for *brain tapping* by commercial enterprises, spy agencies, or terrorists suggests a future where the most private aspects of human existence (one's own thoughts), are subject to surveillance and exploitation (Alohaly 2024). This raises questions regarding the right to mental privacy and the need for informed consent in any BCI application.

In the context of modern warfare, whoever reigns over knowledge will eventually become the ruler of the cyber world (Sharp 2020: 332). The combination of human ingenuity and neuromorphic BCI (nBCI) allows for *data-based targeting* and highly influential cyberattacks. These destructive outputs transform the human into a weapon that disrupts standard combat conventions.

A significant ethical and legal concern arises where traditional warfighters are expected to internally regulate themselves based on established codes, a nBCI warfighter may be incapable of such internal regulation due to the external modulation of their cognitive functions (Sharp 2020: 337).

This lack of autonomy challenges the legal standards for combatants and may provoke states to exercise their inherent right to preventive self-defense to stop such weapons from becoming operational (Sharp 2020: 319). This would probably become more relevant in future types of military BCIs.

A unique complication in the cyberbiosecurity of BCIs is the role of the private sector. Private entities often possess the resources and global talent to develop BCI technology at a pace far exceeding democratic governments, which are slowed by formalities (Sharp 2020: 332). Consequently, non-state actors could soon achieve intellectually dominant cyber capabilities, potentially bypassing the ethical and security oversight typically mandated for state-controlled military technologies and gaining capabilities such as intelligence exploitation or behavioral manipulation.

Regulatory Gaps

Current regulatory and security frameworks suffer from significant gaps when addressing the specific needs of cyberbiosecurity in BCIs. These vulnerabilities often persist due to inadequate cybersecurity procedures, a failure to recognize the value of organizational data, and insufficient attention from equipment manufacturers and software developers (Reed & Dunaway 2019: 13). Current laws do not typically contemplate a warfighter as a weapon, nor do they fully address the unique threat vector of cyberbiosecurity. As Lekatis (2026) notes, the difference between cyberbiosecurity and traditional biosecurity is the threat vector: biosecurity assumes a human actor seeking physical access, whereas cyberbiosecurity deals with digital domain threats like the infiltration of cloud-based platforms and the manipulation of biofabrication processes.

To address these gaps, the following measures are essential for securing the BCI landscape.

Enhanced Security Protocols are a critical need for BCI-specific access control mechanisms, advanced cryptographic techniques, and adversarial defense strategies to protect against signal hijacking (Alohaly 2024). Harmful BCI practices must be identified and restricted by law. This includes ensuring compliance with privacy regulations and establishing clear policies on who has access to neurodata (Alohaly 2024; DeFranco et al. 2019: 58). High transparency in data collection and usage practices is required to maintain user trust. Furthermore, increasing public awareness about the risks associated with BCI technology is vital for individual protection (Alohaly 2024).

What's next?

The relevance of cyberbiosecurity in the context of Brain-Computer Interfaces is a matter of both individual safety and national security. Because BCIs bridge the gap between human thought and digital instruction, they create a new frontier of vulnerability. Even when the target becomes digital,

the consequences can be fundamentally of biological significance (Lekatis 2026). Safeguarding this interface requires a shift in how we treat biology, not just as a physical science, but as a multidisciplinary domain where digital data and physical pathogens (or neural signals) are inextricably interconnected (Cunningham and Geis 2020: 58). Without robust cyberbiosecurity measures, the very technologies intended to enhance human capability could instead be used to compromise the integrity of the human mind and the stability of global security frameworks.

References

Alohaly, Manar (2024): Cybersecurity. The brain computer interface market is growing – but what are the risks? Available online at https://www.weforum.org/stories/2024/06/the-brain-computer-interface-market-is-growing-but-what-are-the-risks/

Cunningham, Marcus A.; Geis, John P. (2020): A National Strategy for Synthetic Biology. In Strategic Studies Quarterly 14 (3), pp. 49–80. Available online at https://www.jstor.org/stable/26937411.

DeFranco, Joseph; DiEuliis, Diane; Giordano, James (2019): Redefining Neuroweapons. Emerging Capabilities in Neuroscience and Neurotechnology. In PRISM 8 (3), pp. 48–63. Available online at https://www.jstor.org/stable/26864276.

DiEuliis, Diane (2019): Key National Security Questions for the Future of Synthetic Biology. In The Fletcher Forum of World Affairs 43 (1), pp. 127–143. Available online at http://www.jstor.org/stable/45289832.

Letakis, George (2026): What is Cyberbiosecurity?. Available online at https://www.cyberbiosecurity.ch/.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., and Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Front. Bioeng. Biotechnol. 6:39. doi: 10.3389/fbioe.2018.00039

Reed, J. Craig; Dunaway, Nicolas (2019): Cyberbiosecurity Implications for the Laboratory of the Future. Front. Bioeng. Biotechnol. 7:182. doi: 10.3389/fbioe.2019.00182.

Sharp, Carolyn (2020): Cognitively Enhanced Humans as Both Warfighters and Weapons of War. In University of Florida Journal of Law & Public Policy 32 (2), Article 4. Available online at https://scholarship.law.ufl.edu/jlpp/vol32/iss2/4/.