# Cognitive Liberty as Critical Infrastructure: A Perspective on Brain-Computer Interfaces (BCIs) Through a Cyberbiosecurity (CBS) Lens

**Zachary Lara[1], Abigail Oppong[2], Celisha Oscar[3], Lucas Potter[4] and Xavier-Lewis Palmer[4]**
[1]Independent Researcher, San Francisco, CA, USA
[2]Makerere University Centre for Artificial Intelligence, Kampala, Uganda
[3]Howard University, Washington D.C., USA
[4]BiosView Labs, Dayton, OH, USA

zglara@gmail.com (Corresponding author)
biosview1@proton.me (Corresponding author)

**Abstract:** Brain-Computer Interfaces (BCIs) increasingly integrate human neurological processes with computational systems and are rapidly emerging as a significant component of cyber-bio-physical systems. However, their development has outpaced the security, governance, and ethical frameworks needed to regulate them effectively. This perspective argues that a significant gap exists between BCI security research and neuro-rights scholarship, particularly in addressing risks to cognitive liberty (CL). We suggest a cyberbiosecurity framework that treats human cognition as a form of critical infrastructure. BCIs, including both consumer wellness devices and implanted medical systems, directly interact with neurological processes linked to cognitive liberty; the right to self-determination over one's mental experiences and brain activity. Unlike many conventional medical technologies, consumer BCIs often operate within fragmented regulatory environments while collecting highly sensitive neural and behavioral data. This lack of oversight expands the potential attack surface of neural data and cognitive processes. Such vulnerabilities may enable manipulative forms of targeted messaging, behavioral conditioning, or cognitive influence. A cyberbiosecurity perspective is necessary because BCIs tightly couple biological and computational systems, creating high-impact security and safety risks. These vulnerabilities span neural interfaces, physiological signal processing systems, software pipelines, and supply chains. One of the most serious risks is the erosion of volitional control, or what we describe as "consent degradation." This may contribute to forms of data violence in which the exploitation of neural data or information asymmetries is used to manipulate, isolate, or condition individuals, thereby undermining liberty and informed decision-making. Their manipulation or disruption through BCI exploitation could affect national security, economic stability, and public health systems. Future BCI governance should therefore prioritize transparency, community-centered design, and context-specific risk assessment. Protecting cognitive and biological integrity should become a central objective of secure and ethical BCI development.

**Keywords:** Brain-computer interfaces (BCI), AI, Cyberbiosecurity (CBS), Consent degradation, Critical infrastructure

## 1. Introduction and Early Considerations

We are in an era of unmatched technological progress, in which the convergence of AI and neurotechnology has outstripped regulatory expectations, creating a governance gap that cybersecurity and legal frameworks are struggling to close. This acceleration presents a fundamental dilemma: What level of care and security is being directed to the humans in this equation? This tension is captured in an exchange between two advanced machines in Iain M. Banks' *Look to Windward* regarding the ability to probe a biological brain: *"All it is is looking inside an animal brain... it is so easy... That is why the not-doing of it is probably the most profound manner in which we honor our biological progenitors. This prohibition is a mark of our respect"* (Banks, 2001). This fictional respect highlights the real-world vulnerability of the "unassailable fortress" of the mind, which is now susceptible to external control via neural engineering (Ienca and Andorno, 2017). As BCIs provide unprecedented insight into the emotional and physiological workings of humans, we must address the loss of agency created when third parties gain access to indicators of thought (Kim, 2023; Farahany, 2023). Securing BCI as critical infrastructure is therefore a prerequisite for upholding fundamental neuro-rights. The convergence of AI and neurotechnology is not a linear progression but an accelerating complex system, as Figure 1 illustrates, tracing the shift from the attention economy to today's cyber-bio-physical systems.

This inquiry integrates three foundational pillars: (1) cyberbiosecurity (CBS), addressing security risks at the intersection of biological and computational systems (Peccoud et al., 2018; Murch et al., 2018; George, 2019); (2) cognitive liberty, the preservation of mental self-determination and autonomy over cognitive processes (Bublitz, 2013; Farahany, 2023); and (3) neuro-rights, a framework safeguarding mental integrity, neural data privacy, and psychological continuity against unauthorized neurotechnological intrusion (Ienca and Andorno, 2017; Borbón and Ramírez-Gómez, 2024). We further employ cognitive Infrastructure as an analytical framework. Human cognitive capacity, specifically perception, judgment, and volition, functions as the fundamental node of all high-consequence systems. This framework, distinct from the legal designation of 'Critical Infrastructure' in Section 5, posits that cognitive integrity is the essential prerequisite for systemic

resilience. Safeguarding this architecture is therefore a systemic security imperative, rather than solely a privacy concern.

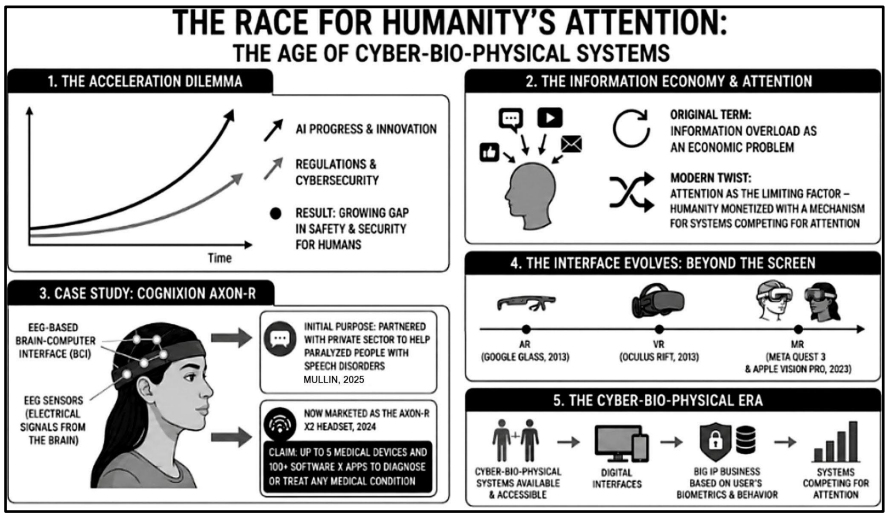


**Figure 1: This figure illustrates the "Acceleration Dilemma," mapping the widening gap between rapid AI and neurotechnology innovation and existing regulatory and cybersecurity frameworks. It highlights the shift from medical utility to the monetization of attention and behavioral data**

### 1.1 Core Concepts and Design

Herbert A. Simon provided a foundational economic account of attention scarcity, arguing that information abundance creates a corresponding scarcity of human attention and therefore a problem of allocation (Simon, 1971). In the discussion accompanying Simon's contribution, Karl W. Deutsch termed this an "economy of

attention" in which limited human attention becomes a resource over which information providers and commercial actors compete (Goldhaber, 1997; Davenport and Beck, 2001). Williams (2018) extends this account beyond economic scarcity, examining how technologically mediated competition for attention affects individual agency, autonomy, and self-directed attention.

Contemporary digital markets have further transformed attention into an object of measurement, prediction, and optimization. Attention-based business models incentivize firms to use behavioral feedback, interface design, and algorithmic systems to capture engagement and shape the allocation of attention (Bhargava and Velasquez, 2021; O'Reilly, Strauss and Mazzucato, 2024). This dynamic is evident in platform marketplaces such as Amazon, where algorithmic ranking and information architecture may influence the distribution of user attention and create opportunities for rent extraction (Strauss, O'Reilly and Mazzucato, 2024). Emerging immersive, gaze-responsive, biometric, and neuroadaptive interfaces may deepen this dynamic by shifting from systems that primarily infer attention from observable behavior to systems that sense and respond to perceptual, physiological, or cognitive states.

The shift from screen-based to bio-adaptive interfaces necessitates a new regulatory focus: moving beyond mere attention competition to preventing unauthorized cognitive observation or intervention. Consequently, the attention economy now deeply intersects with neuro-rights,specifically: autonomy, mental privacy, and cognitive liberty (Williams, 2018; Ienca and Andorno, 2017; Bozkir et al., 2025).

## 2. BCIs as Cyberbiosecurity Systems

Brain-Computer Interfaces (BCIs) are complex cyber-bio-physical (CBP) systems rather than isolated medical or digital devices. Their architecture integrates the "bio" component (sensitive neural signals and the human subject) with the "physical" element (electrodes, hardware, and acquisition environment) and the "cyber" layer (signal-processing algorithms and network protocols). This tight systemic coupling introduces unique vectors for compromise, necessitating a holistic defense strategy that transcends conventional medical device oversight.

The shift toward integrated systems is exemplified by devices like Cognixion's Axon-R. Initially developed with Apple Vision to integrate EEG-based BCIs with Mixed Reality (MR) for those with speech disorders, the technology has evolved into a broader consumer-facing platform (Mullin, 2025). Importantly, the platform

carried a disclaimer that it was for research use only (Cognixion, 2025). This transition from a targeted medical tool to an open consumer interface illustrates the emergence of cyber-bio-physical systems in which neural data is collected outside traditional clinical governance.

Safeguarding neural autonomy requires the formal establishment of neuro-rights - safeguards for mental integrity, autonomy, and neural data privacy that counter security risks even absent data exfiltration (Farahany, 2023; Favero et al., 2026; UNESCO, 2025). As cognitive liberty underpins the capacity for learning, reasoning, and democratic participation, these safeguards are not merely ethical choices but structural prerequisites for agency in AI-integrated environments. Consequently, we contend that cognitive Liberty must be formally recognized as Critical Infrastructure. This framing elevates neuro-sovereignty from an ethical concern to an operational security mandate,requiring governance that secures the cognitive substrate against manipulation and unauthorized access.

### 2.1 Overview of BCI Architectures and Data Flows

The term 'brain-computer-interface' (BCI) was coined by Jacques Vidal (1973) at UCLA in 1973, theorizing that subjects could receive computer influence and respond with brain variations detectable by EEG sensors. This built on earlier work, including Berger (1931), Marshall et al. (1943), and Adey (1966), which laid the foundation for more complex inquiries. Since then, advances in BCI development and computing have enabled improved signal resolution and interpretation. Closed-loop direct brain stimulation has advanced to treat epilepsy, relieve depression, and restore speech in neurological disorders. This combination of computing, communication, biological interaction, and physical systems constitutes a cyber-bio-physical system (CBPS) at a level where biological manipulation is not merely possible but demonstrated.

BCI research dates to the early 1970s and, for much of its history, was concentrated primarily in research, clinical, and assistive applications, with consumer-facing uses expanding more recently (Kawala-Sterniuk et al., 2021). For BCIs that meet the statutory definition of a “cyber device,” Section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act) imposes cybersecurity requirements on covered premarket submissions (United States Congress, 2022). Under Section 524B, a cyber device is one that includes software authorized by the sponsor, can connect to the Internet, and contains technological characteristics that could be vulnerable to cybersecurity threats (United States Congress, 2022; U.S. Food and Drug Administration, 2026a). FDA guidance for implanted BCIs separately recognizes software, wireless communications, risk management, and cybersecurity as relevant considerations in device development and evaluation (U.S. Food and Drug Administration, 2021). At the consumer end of the spectrum, certain neurotechnologies marketed for general wellness may fall outside the statutory definition of a medical device or may not be subject to CDRH regulatory oversight (U.S. Food and Drug Administration, 2026b). Such devices can nevertheless collect and process substantial amounts of sensitive neural and physiological information, creating privacy risks within a broader commercial data ecosystem in which sensitive mental health information is marketed and sold by data brokers (Fontanillo Lopez, Li and Zhang, 2020; Kim, 2023).

The Quality Management System Regulation (QMSR) adopts ISO 13485:2016 as the primary standard for FDA-regulated medical-device manufacturers, alongside additional FDA-specific requirements (U.S. Food and Drug Administration (FDA), 2024). Manufacturers must adapt their implementation to their specific organizational context and regulatory obligations (Abuhav, 2018; Kulkarni and Vemuri, 2014). For consumer neurotechnology, the threshold issue is whether a product's claims qualify it as a medical device or a low-risk general wellness product, which dictates device classification, pre-market, and post-market requirements (U.S. Food and Drug Administration (FDA), 2019; U.S. Food and Drug Administration (FDA), 2026b). Data-governance assessments must navigate complex federal and state requirements; for instance, California’s SB 1223 (2024) proposes classifying neural data as sensitive information under the California Consumer Privacy Act (California State Senate, 2024). Ultimately, regulatory requirements depend on product usage, classification, data nature, and jurisdiction.

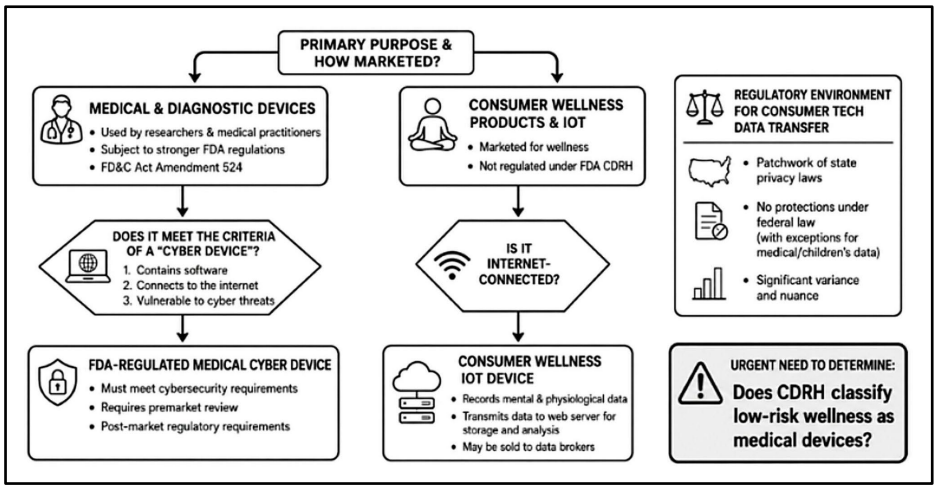


**Figure 2: Distinction between BCIs as conventional medical devices or IoT**

### 2.2 Relevance of Cyberbiosecurity Concepts (Tight Coupling, High Consequence, Interface Risk)

Cyberbiosecurity has been established in academic discourse since 2018, with Peccoud et al. (2018) highlighting the security implications of biotechnology's increasing cyber-physical integration and Murch et al. (2018) formalizing cyberbiosecurity as an intersection of cybersecurity, cyber-physical security, and biosecurity. Although BCI cybersecurity is an established area of study (López Bernal et al., 2020; López Bernal et al., 2021), comparatively little work explicitly frames BCIs as a cyberbiosecurity problem (Greenbaum, 2023; Botes, 2024). This underrepresentation and the increasing convergence of neurotechnology and digital systems are heightening regulatory challenges, especially as legal and technological boundaries blur. U.S. regulatory fragmentation illustrates the problem: FDA guidance addresses implanted BCIs for paralysis or amputation while excluding non-implanted systems from its scope (FDA, 2021). Loper Bright Enterprises v. Raimondo (2024), which ended Chevron deference, may further complicate emerging-technology governance by increasing the importance of explicit statutory authority where regulatory mandates have not anticipated such convergence. Given that BCIs and their requisite computing infrastructure are integral to the healthcare sector and the broader bioeconomy, they cannot be overlooked as crucial components that are susceptible to malicious agent attack surfaces. Data obtained from a direct attack on an EEG Device or from recorded data could result in loss of personal agency, the revelation of confidential material, physical harm to the individual, and simple responses to stimuli cross-referenced to geodata.

An important driver of exfiltrating BCI-derived data is the refinement of targeted social engineering campaigns: granular cognitive information enhances the efficacy of multi-vector cyber-attacks. Frank et al. (2017) reveal that subliminal interception of subjects' mental concepts is possible within short windows. Ransomware attacks have repeatedly disrupted hospital infrastructure and compromised sensitive health information, while the growing connectivity of medical and implantable devices expands the healthcare attack surface (Cartwright, 2023; Munoz Cornejo, Lee and Russell, 2024). Although analogous cybersecurity vulnerabilities have been identified in BCIs, their intersection with ransomware remains largely prospective. The hospital sub-domain of the bioeconomy has long been targeted, including examples such as the "Tardigrade" malware aimed at vaccine manufacturing and unchecked third-party IoT medical devices compromised as malware entry points into hospitals (Affia et al., 2023; Elgabry and Johnson, 2024). The assumption that healthcare facilities are of slight interest to criminal organizations is clearly outdated. This expanded hospital sector needs comprehensive protection, which would benefit from integrated, multi-domain security solutions capable of preventing billions in losses.

## 3. BCI Vulnerabilities Across System Layers

Brain-Computer Interfaces (BCIs) face significant security and privacy risks across multiple layers of vulnerability, including neurological vulnerabilities; signal processing and algorithmic manipulation; system, network, and supply-chain risks; and human-in-the-loop and consent degradation issues, as shown in Figure 3.

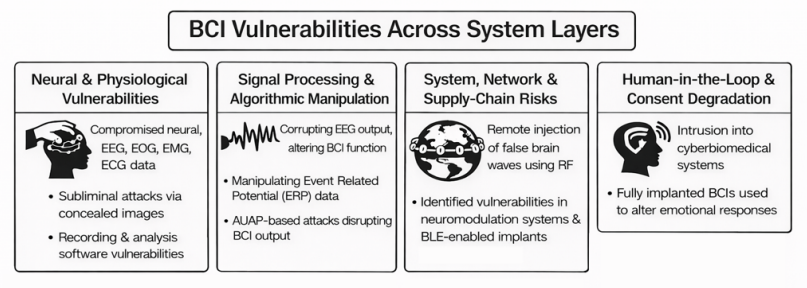


**Figure 3: Simplified presentations of BCI Vulnerabilities Across System Layers**

These threats emerge at the neural and physiological data layer, where wearable architectures acquire and wirelessly transmit biosignals including EEG, EOG, EMG, and ECG (Lesaja and Palmer, 2020; Apple Inc., 2023). Neural data may expose sensitive information if intercepted or improperly analysed, including aspects of users' activities, feelings, and emotional states (Li et al., 2015). Subliminal visual stimuli embedded within screen content have also been shown to enable probabilistic inference of private information from EEG responses without users' conscious awareness (Frank et al., 2017). At the software layer, remotely exploitable code-execution and denial-of-service vulnerabilities have been identified in networked clinical EEG systems, creating risks to the integrity and availability of EEG-related workflows (Cisco Talos, 2018). At the signal-processing and machine-learning layer, Attention-guided Universal Adversarial Perturbations (AUAP) have been shown to induce misclassification in EEG-based BCI models, with potential downstream consequences for device control and clinical interpretation (Zhong et al., 2025).

System, network, and supply-chain risks add another layer of concern. Experimental research has demonstrated that radio-frequency signals can inject false data into EEG acquisition systems and alter the outputs of EEG-based brain–computer interfaces (Apple Inc., 2023; Armengol-Urpi, Kovacs and Sarma, 2023). Independent security advisories have also documented vulnerabilities in clinician-programming systems supporting neurological implants (CISA, 2018) and in Bluetooth Low Energy communications used by certain implantable medical devices (FDA, 2020). These risks extend into digital manufacturing, where malicious hardware or software modifications may be introduced during production or through supply chains, creating additional pathways for compromise across the device lifecycle (Basu Roy et al., 2023). Finally, human-in-the-loop and consent-degradation issues involve validated intrusion into cyberbiomedical systems (Li et al., 2015; Conti et al., 2015), suggesting that fully implanted BCIs, such as Neuralink (Musk and Neuralink, 2019), could influence an individual's emotional response and reduce personal agency. These layered, complex security and privacy vulnerabilities underscore the critical, urgent need for robust frameworks to protect both cognitive liberty and neuro-rights in the age of cyberbiomedical systems (The MITRE Corporation, 2018). These are illustrated in Table 1 below.

**Table 1: Representative vulnerabilities across BCI system layers and their potential security implications**

Condensed BCI Vulnerability Table

| System layer | Vulnerability | Evidence/Example | Significance |
|---|---|---|---|
| **Neural-data acquisition** | Signal spoofing or injection | Synthetic noise and fake-P300 signals disrupted a laboratory P300 BCI (Mezzina, Annese and De Venuto, 2021). | Manipulated signals may alter inferred user intent or system output. |
| **Machine learning** | Adversarial inputs | Small perturbations reduced the accuracy of several EEG-based CNN classifiers (Zhang and Wu, 2019). | Incorrect classification may generate unintended commands. |
| **Privacy and cognitive inference** | Extraction of sensitive information | EEG responses enabled partial PIN-code inference under controlled conditions (Lange et al., 2018). | Neural data may reveal information beyond its original purpose. |
| **Software and networks** | Remote compromise | Vulnerabilities in Natus NeuroWorks permitted potential code execution or denial of service (Cisco Talos, 2018). | Attacks could affect neurological-data confidentiality, integrity and availability. |
| **Implant and device security** | Malicious neural stimulation | Simulated flooding and scanning attacks disrupted modelled neural signaling (López Bernal et al., 2020). | Cyberattacks may theoretically produce physiological consequences. |
| **Cross-layer wearable systems** | Combined platform, communication and model attacks | Testing of Muse, NeuroSky and OpenBCI platforms identified vulnerabilities across multiple attack vectors (Tarkhani et al., 2022). | Security must address the complete BCI ecosystem rather than isolated components. |

Please note that cited studies include laboratory experiments, simulations, technical advisories and preprint research; they should not all be interpreted as evidence of successful real-world attacks.

## 4. Discussion: Cognitive Liberty and Neuro-rights

The concept of cognitive liberty is becoming increasingly vital in the age of neurotechnology, necessitating the formal establishment of related neuro-rights. These rights aim to protect an individual's autonomy over their own mind and mental processes. A central tenet is the freedom to decide whether to use neurotechnologies and to control one's own thoughts, mental privacy, and mental integrity. While Farahany (2023) defines cognitive liberty, framing it in terms of neuro-rights for Communities, aligned with local politics and cultural practices, is a crucial step for ethical governance as BCIs and other neurotechnologies advance rapidly. This includes the development of "neuro-rights" - a new category of rights intended to safeguard cognitive liberty, neural data privacy, mental integrity, autonomy, psychological continuity, and others (Borbón and Ramírez-Gómez, 2024).

### 4.1 Limitations of Existing Ethical and Legal Frameworks

The rapid evolution of neurotechnology and brain-computer interfaces (BCIs) exposes the obsolescence of existing ethical and legal safeguards. Current regulatory frameworks, designed for analog-era data, lack the mechanisms to protect individual autonomy, mental privacy, and neural integrity against direct interface access. Bridging this governance gap requires codifying “neuro-rights” to safeguard the cognitive substrate of selfhood, including psychological continuity and the privacy of neural data. This codification must be sensitive to the diverse cultural and political contexts in which these technologies operate to ensure meaningful protection as neurotechnology matures. Figure 4 supplies a map.

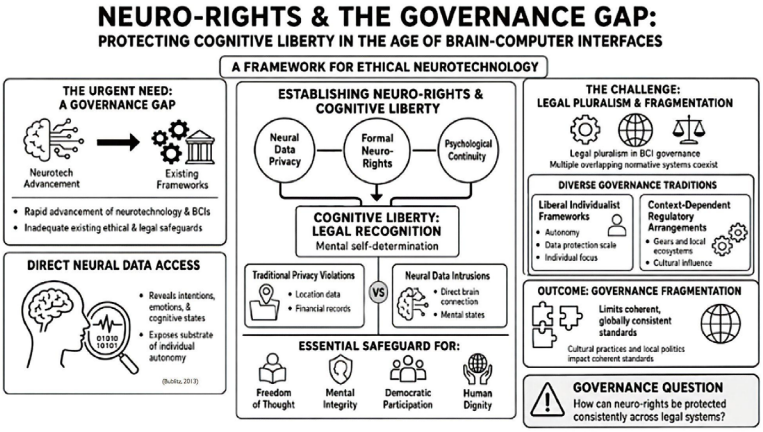


**Figure 4: Neuro-rights and the governance gap in brain-computer interfaces**

Additionally, while the concept of cognitive liberty is gaining traction, existing ethical and legal frameworks are inadequate for the unique challenges posed by neurotechnologies. These older structures were not designed to protect an individual's cognitive liberty, necessitating formal recognition of "neuro-rights”. The authors suggest that this structural inadequacy may be compounded by the post-Chevron administrative-law environment established by Loper Bright Enterprises v. Raimondo (2024), which ended mandatory judicial deference to agency interpretations and placed greater responsibility on courts to determine statutory meaning independently. Although agency expertise may remain persuasive, this shift underscores the necessity of ongoing cooperation among neuroscientific, cybersecurity, and legal sectors to address emerging challenges involving neural data, closed-loop stimulation, or cognitive inference. Neither adjudication nor legacy statute alone appear sufficient, so effective BCI regulation depends on formalized, iterative collaboration that builds confidence in governance capable of evolving with technological advances.

The legal recognition of cognitive liberty is essential, as emerging neurotechnologies provide avenues for intrusion that existing frameworks may not address. Unlike other traditional privacy violations involving external information, neural data may reveal intentions, emotions, and cognitive states, exposing the very foundation on which individuals practice autonomy and agency. Bublitz (2013) conceptualizes cognitive liberty as a form of mental self-determination, emphasizing that interference with cognitive processes constitutes a distinct category of rights violation. Similarly, Ienca and Andorno (2017) argue that existing human rights protections may be insufficient to respond to these emerging challenges. Subsequently, cognitive liberty goes beyond merely being an extension of privacy rights but also as a safeguard for freedom of thought, mental integrity, and the conditions necessary for democratic participation and human dignity. Also, another key limitation is the reliance

on a universal model of rights, autonomy, and consent. In practice, the governance of BCI operates within a context of legal pluralism, where multiple overlapping normative systems coexist and interact (Griffiths, 1986). Shaped by diverse institutional, customary, and transnational regulatory orders, legal pluralism recognizes that the law is not singular and, within this environment, the regulatory approaches to BCIs reflect differing governance traditions, ranging from the liberal individualist frameworks focusing on autonomy and data protection to more context-dependent approaches of coherent and globally consistent standards for neurotechnology regulation (Bennett and Raab, 2017).

### 4.2 Security Relevance: Harms With and Without Data Exfiltration

Adverse outcomes may arise not only from unauthorized data extraction but also from decisions about which data are collected, retained, interpreted, omitted, or withheld. The concept of data violence captures harms produced by data practices and technologies, including how sociotechnical systems can reproduce or intensify unequal relations through processes of representation, classification, inclusion, and exclusion (Hoffmann, 2018, 2019). Related work in data justice places such harms within broader relations of extraction, domination, and unequal participation in data infrastructures (Vera et al., 2019); more recent research extends data violence to networked environments (Kayış, 2025). Social harm can be amplified through precise data harvesting and targeted (Potter and Palmer, 2024). In BCI contexts, neural data may enable inferences about cognitive, affective, or behavioral states, creating risks to mental privacy and discriminatory or harmful decision-making (Ienca and Andorno, 2017; Jwa and Poldrack, 2022). Data violence stems from biased collection or interpretation that unfairly classifies individuals based on sensing modality, data quality, and usage context. The 2026 Bondu incident, where inadequate controls exposed transcripts of 50,000 children's conversations, highlights the risks of persistent data retention (Greenberg, 2026). While not a neuro-specific case, this illustrates how highly personal datasets pose risks that exceed their original purpose. Thus, BCIs can intensify by generating longitudinal neural data that are susceptible to secondary profiling (Lesaja and Palmer, 2020). Beyond privacy loss, this creates 'interpretive asymmetry,' where controllers exercise disproportionate influence over how individuals are represented. Consequently, BCI governance must address data minimization, retention, access, and mechanisms for contesting consequential classifications.

### 4.3 Security Implications for Agency and Cognitive Control

Beyond privacy violations, surveillance asymmetries, and data-driven exclusion lies a more direct neurosecurity risk: compromise of agency. In bidirectional BCIs and neuromodulation systems, unauthorized or coercive alteration of stimulation may affect neural processes involved in affect, motivation, action, or decision-making, creating harms beyond the confidentiality or integrity of neural data (Pycroft et al., 2016; Pugh et al., 2018). Where technology mediates the relationship between intention and action, such interference may also compromise users' control over BCI-mediated outcomes (Mehta, 2025). Building on existing accounts of data violence and data-justice harms (Hoffmann, 2018; Vera et al., 2019), we extend the concept to interventions that affect not only how individuals are represented through data, but also how their agency is exercised. Even without dramatic changes to personality, interference affecting attention, affect, motivation, or other decision-relevant states may implicate autonomy and mental integrity (Pugh et al., 2018). Recognizing agency manipulation as a distinct neurosecurity concern, shifts BCI governance toward preserving voluntary control, cognitive continuity, and the revocability of intervention. For systems capable of stimulation, safeguards should restrict stimulation authority, authenticate parameter changes, and preserve meaningful user control. Under this framework, BCI security must protect not only neural data and device operation but also the continuity of human self-governance.

## 5. Cognitive Liberty as Critical Infrastructure

### 5.1 Analogy to Traditional Critical Infrastructure Systems

Section 1016(e) of the USA PATRIOT Act of 2001, codified at 42 U.S.C. § 5195c(e), defines critical infrastructure as physical or virtual systems and assets "so vital to the United States" that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof (United States Congress, 2001). Nevertheless, Critical infrastructure operation depends on human cognition, attention, perception, judgment, memory, and decision-making, which human reliability research identifies as integral to the safe operation of complex infrastructure systems (Sun et al., 2020). We therefore propose that such capacities constitute a form of critical human infrastructure, whose degradation or manipulation may compromise the systems they support. From this perspective, cognitive liberty (CL) is both a

rights-based concern and a security interest protecting the cognitive autonomy on which critical-infrastructure resilience depends (Bublitz, 2013; Ienca and Andorno, 2017). Figure 5 presents these key concepts.

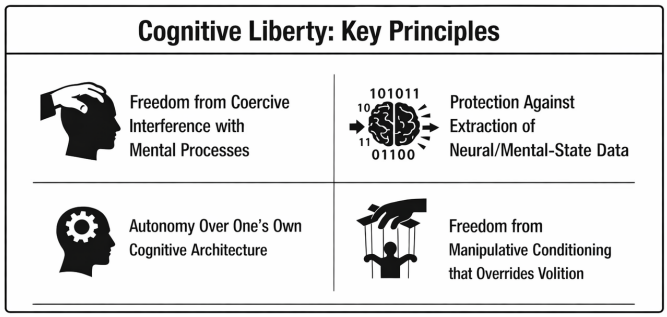


**Figure 5: Graphic that presents simplified presentations of (CL) Key Principles**

Establishing robust protections requires a holistic approach that integrates sociological considerations, including neurodiversity. This framework should not be viewed as static; it requires continuous, iterative refinement to reflect evolving empirical insights into human cognitive architectures and the interplay between biological substrates and computational interfaces.

## 6. Conclusion

The integration of Brain-Computer Interfaces (BCIs) demands a shift from universalist regulatory posturing toward contextualized, principle-based governance. Optimal transparency, inclusive design, and proactive auditing are essential to mitigate the risks of exploitation inherent in existing power stratifications. By adopting the curb-cut effect, where design for marginalized populations yields broader societal utility, we can transform BCI deployment from a site of vulnerability into a mechanism for collective resilience and cognitive liberation. Ultimately, the human mind constitutes a foundational node of critical infrastructure, demanding protections commensurate with those afforded to physical or digital systems. Prioritizing cognitive and biological integrity is no longer an ethical adjunct, but it is a mandatory security vector for a resilient bioeconomy. Safeguarding this cognitive substrate is the primary prerequisite for AI-integrated societies. Ultimately, national security and economic prosperity are inextricably linked to preserving cognitive agency within the expanding cyber-biological domain.

**Ethics Declaration:** Ethical approval through IRB is not applicable.

**AI Declaration:** AI tools in ChatGPT, Claude, Google Docs/Gemini, and Grammarly were employed to organise pre-written material and develop figures.

## References

Abuhav, I. (2018) ISO 13485:2016: A complete guide to quality management in the medical device industry. 2nd edn. Boca Raton, FL: CRC Press.

Adey, W. R. (1966) 'Progress in Physiological Psychology', in Stellar, E. and Sprague, J.M. (eds.) Progress in Physiological Psychology, pp. 1–43. New York: Academic.

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X.L. (2023) 'IoT health devices: exploring security risks in the connected landscape', IoT, 4(2), pp. 150-182.

Apple Inc. (2023) Biosignal sensing device using dynamic selection of electrodes. US Patent Application US20230225659A1.

Armengol-Urpi, A., Kovacs, R. and Sarma, S.E. (2023) 'Brain-hack: Remotely injecting false brain-waves with rf to take control of a brain-computer interface', in Proceedings of the 5th Workshop on CPS&IoT Security and Privacy, pp. 53-66.

Banks, I.M. (2001) Look to Windward. London: Simon and Schuster.

Basu Roy, P., Bhargava, M., Chang, C.-Y., Hui, E., Gupta, N., Karri, R. and Pearce, H. (2023) 'A survey of Digital Manufacturing Hardware and Software Trojans', arXiv preprint, arXiv:2301.10336. doi:10.48550/arXiv.2301.10336.

Berger, H. (1931) 'Über das elektrenkephalogramm des menschen', Archiv für Psychiatrie und Nervenkrankheiten, 94(1), pp. 16-60.

Bennett, C.J. and Raab, C.D. (2017) The Governance of Privacy: Policy Instruments in Global Perspective. 2nd edn. Cambridge, MA: MIT Press.

Bhargava, V.R. and Velasquez, M. (2021) 'Ethics of the Attention Economy: The Problem of Social Media Addiction', Business Ethics Quarterly, 31(3), pp. 321–359. doi:10.1017/beq.2020.32.

Borbón, D. and Ramírez-Gómez, J.A. (2024) 'Between politics and scholarship: the (un) settled debate over neurorights', Frontiers in Political Science, 6, p. 1335561.

Botes, M. (2024) 'Enhancing Cyberbiosecurity in Brain-Computer Interfaces: Regulatory, Ethical, and Technological Perspectives', Datenschutz und Datensicherheit – DuD, 48(12), pp. 775–779. doi:10.1007/s11623-024-2016-9.

Bozkir, E., Bühler, B., Wu, X., Kasneci, E., Bauer, L. and Cranor, L.F. (2025) 'The impact of device type, data practices, and use case scenarios on privacy concerns about eye-tracked augmented reality in the United States and Germany', Journal of Cybersecurity, 11(1), tyaf036. doi:10.1093/cybsec/tyaf036.

Bublitz, C. (2013) 'My mind is mine!? Cognitive liberty as a legal concept', in Hildt, E. and Franke, A.G. (eds.) Cognitive Enhancement: An Interdisciplinary Perspective. Dordrecht: Springer, pp. 233–264. doi:10.1007/978-94-007-6253-4_19.

California State Senate (2024) Senate overwhelmingly approves nation's strongest neurorights bill. 21 May. https://sd13.senate.ca.gov/news/press-release/may-21-2024/senate-overwhelmingly-approves-nations-strongest-neurorights-bill.

Cartwright, A.J. (2023) 'The elephant in the room: cybersecurity in healthcare', Journal of Clinical Monitoring and Computing, 37(5), pp. 1123–1132. doi:10.1007/s10877-023-01013-5.

Cisco Talos (2018) 'Vulnerability Spotlight: Natus NeuroWorks Multiple Vulnerabilities', Talos Intelligence Blog, 4 April. https://blog.talosintelligence.com/vulnerability-spotlight-natus/.

Cognixion (2025) Axon-R: wearable brain-computer interface platform. https://axon-r.cognixion.com/.

Conti, M., Mancini, L.V., Spolaor, R. and Verde, N.V. (2015) 'Can't you hear me knocking: Identification of user actions on android apps via traffic analysis', in Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, pp. 297-304.

Cybersecurity and Infrastructure Security Agency (CISA) (2018) 'Medtronic N'Vision Clinician Programmer (Update A)', ICS Medical Advisory ICSMA-18-137-01, 12 July.

Davenport, T.H. and Beck, J.C. (2001) The Attention Economy: Understanding the New Currency of Business. Boston: Harvard Business School Press.

Elgabry, M. and Johnson, S. (2024) 'Cyber-biological convergence: a systematic review and future outlook', Frontiers in Bioengineering and Biotechnology, 12, p. 1456354. doi:10.3389/fbioe.2024.1456354.

Farahany, N.A. (2023) The battle for your brain: defending the right to think freely in the age of neurotechnology. New York: St. Martin's Press.

Favero, L., Pérez-Ortiz, J.A., Käser, T. and Oliver, N. (2026) AI in Education Beyond Learning Outcomes: Cognition, Agency, Emotion, and Ethics. arXiv Preprint, arXiv:2602.04598. doi:10.48550/arXiv.2602.04598.

Fontanillo Lopez, C.A., Li, G. and Zhang, D. (2020) 'Beyond technologies of electroencephalography-based brain-computer interfaces: A systematic review from commercial and ethical aspects', Frontiers in Neuroscience, 14, p. 611130. doi:10.3389/fnins.2020.611130.

Frank, M., Hwu, T., Jain, S., Knight, R.T., Martinovic, I., Mittal, P., Perito, D., Sluganovic, I. and Song, D. (2017) 'Using EEG-based BCI devices to subliminally probe for private information', in Proceedings of the 2017 on Workshop on Privacy in the Electronic Society, pp. 133-136.

George, A.M. (2019) 'The national security implications of cyberbiosecurity', Frontiers in Bioengineering and Biotechnology, 7, p. 51. doi:10.3389/fbioe.2019.00051.

Greenbaum, D. (ed.) (2023) Cyberbiosecurity: A new field to deal with emerging threats. Cham: Springer. doi:10.1007/978-3-031-26034-6.

Greenberg, A. (2026) 'An AI toy exposed 50,000 logs of its chats with kids to anyone with a Gmail account', Wired, 29 January.

Griffiths, J. (1986) 'What is legal pluralism?', Journal of Legal Pluralism and Unofficial Law, 18(24), pp. 1–55.

Goldhaber, M.H. (1997) 'The Attention Economy and the Net', First Monday, 2(4). doi:10.5210/fm.v2i4.519.

Hoffmann, A. L. (2018) 'Data Violence and How Bad Engineering Choices Can Damage Society'. https://medium.com/s/story/data-violence-and-how-badengineering-choices-can-damage-society-39e44150e1d4.

Hoffmann, A. L. (2019) 'Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse', Information, Communication & Society, 22(7), pp. 900–915. doi:10.1080/1369118x.2019.1573912.

Jwa, A.S. and Poldrack, R.A. (2022) 'Addressing privacy risk in neuroscience data: from data protection to harm prevention', Journal of Law and the Biosciences, 9(2), lsac025. doi:10.1093/jlb/lsac025.

Kawala-Sterniuk, A., Browarska, N., Al-Bakri, A., Pelc, M., Zygarlicki, J., Sidikova, M., Martinek, R. and Gorzelanczyk, E.J. (2021) 'Summary of over fifty years with brain-computer interfaces—A review', Brain Sciences, 11(1), p. 43. doi:10.3390/brainsci11010043.

Kayış, H.H. (2025) 'Data violence in networked environments: A study on user experience', Yeni Medya, 18, pp. 106–123. doi:10.55609/yenimedya.1626763.

Kim, J. (2023) Data Brokers and the Sale of Americans' Mental Health Data: The Exchange of Our Most Sensitive Data and What It Means for Personal Privacy. Durham, NC: Duke University, Sanford School of Public Policy.

Kulkarni, B. and Chandra Vemuri, R. (2014) 'Role of Quality Management System (QMS) for effective regulatory compliance', Applied Clinical Research, Clinical Trials and Regulatory Affairs, 1(3), pp. 157-168.

Lange, J., Massart, C., Mouraux, A. and Vandergheynst, P. (2018) 'Side-channel attacks against the human brain: the PIN code case study (extended version)', Brain Informatics, 5, p. 12. doi:10.1186/s40708-018-0090-1.

Ienca, M. and Andorno, R. (2017) 'Towards new human rights in the age of neuroscience and neurotechnology', Life Sciences, Society and Policy, 13(1), p. 5. doi:10.1186/s40504-017-0050-1.

Lesaja, S. and Palmer, X.-L. (2020) 'Brain-computer interfaces and the dangers of neurocapitalism', arXiv preprint, arXiv:2009.07951.

Li, Q., Ding, D. and Conti, M. (2015) 'Brain-computer interface applications: Security and privacy challenges', in 2015 IEEE Conference on Communications and Network Security (CNS), pp. 663-666.

Loper Bright Enterprises v. Raimondo (2024) 603 U.S. 369.

López Bernal, S., Huertas Celdrán, A., Fernández Maimó, L., Barros, M.T., Balasubramaniam, S. and Martínez Pérez, G. (2020) 'Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling', IEEE Access, 8, pp. 152394–152408. doi:10.1109/ACCESS.2020.3017394.

López Bernal, S., Huertas Celdrán, A., Martínez Pérez, G., Barros, M.T. and Balasubramaniam, S. (2021) 'Security in brain-computer interfaces: State-of-the-art, opportunities, and future challenges', ACM Computing Surveys, 54(1), Article 11, pp. 1–35. doi:10.1145/3427376.

Marshall, W.H., Talbot, S.A. and Ades, H.W. (1943) 'Cortical response of the anesthetized cat to gross photic and electrical afferent stimulation', Journal of Neurophysiology, 6(1), pp. 1-15.

Mehta, D. (2025) 'Brain-Computer Interface tool use and the Contemplation Conundrum: a blueprint of mental action, agency, and control', Oxford Open Neuroscience, 4, kvaf002. doi:10.1093/oons/kvaf002.

Mezzina, G., Annese, V.F. and De Venuto, D. (2021) 'A cybersecure P300-based brain-to-computer interface against noise-based and fake P300 cyberattacks', Sensors, 21(24), p. 8280. doi:10.3390/s21248280.

Mullin, E. (2025) 'This startup wants to put its brain-computer interface in the Apple Vision Pro', Wired, 1 October. https://www.wired.com/story/this-startup-wants-to-put-its-brain-computer-interface-in-the-apple-vision-pro/.

Munoz Cornejo, G., Lee, J. and Russell, B.A. (2024) 'A thematic analysis of ransomware incidents among United States hospitals, 2016–2022', Health and Technology, 14, pp. 1059–1070. doi:10.1007/s12553-024-00890-3.

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', Frontiers in Bioengineering and Biotechnology, 6, p. 39. doi:10.3389/fbioe.2018.00039.

Musk, E. and Neuralink (2019) 'An integrated brain-machine interface platform with thousands of channels', Journal of Medical Internet Research, 21(10), e16194. doi:10.2196/16194.

O'Reilly, T., Strauss, I. and Mazzucato, M. (2024) 'Algorithmic attention rents: A theory of digital platform market power', Data & Policy, 6, e6. doi:10.1017/dap.2024.1.

Potter, L. and Palmer, X.L. (2024) 'Social Murder in Another Century', Journal of Information Warfare, 23(4), pp. 45-56.

Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G. and Raman, S. (2018) 'Cyberbiosecurity: from naive trust to risk awareness', Trends in Biotechnology, 36(1), pp. 4-7. doi:10.1016/j.tibtech.2017.10.012.

Pugh, J., Pycroft, L., Sandberg, A., Aziz, T. and Savulescu, J. (2018) 'Brainjacking in deep brain stimulation and autonomy', Ethics and Information Technology, 20(3), pp. 219–232. doi:10.1007/s10676-018-9466-4.

Pycroft, L., Boccard, S.G., Owen, S.L.F., Stein, J.F., Fitzgerald, J.J., Green, A.L. and Aziz, T.Z. (2016) 'Brainjacking: implant security issues in invasive neuromodulation', World Neurosurgery, 92, pp. 454–462. doi:10.1016/j.wneu.2016.05.010.

Simon, H. A. (1971) "Designing Organizations for an Information-rich World", in Greenberger, M. (ed.) Computers, Communications, and the Public Interest, pp. 37–72. Baltimore: Johns Hopkins Press.

Strauss, I., O'Reilly, T. and Mazzucato, M. (2024) "Amazon's Algorithmic Rents: The economics of information on Amazon". UC Law Science and Technology Journal, 15(2), p. 203.

Sun, Z., Xing, J., Tang, P., Cooke, N.J. and Boring, R.L. (2020) 'Human reliability for safe and efficient civil infrastructure operation and maintenance – A review', Developments in the Built Environment, 4, p. 100028. doi:10.1016/j.dibe.2020.100028.

Tarkhani, Z., Qendro, L., O'Connor Brown, M., Hill, O., Mascolo, C. and Madhavapeddy, A. (2022) 'Enhancing the security & privacy of wearable brain-computer interfaces', arXiv preprint, arXiv:2201.07711. doi:10.48550/arXiv.2201.07711.

The MITRE Corporation (2018) Rubric for applying CVSS to medical devices. https://www.mitre.org/sites/default/files/2021-11/pr-18-2208-rubric-for-applying-cvss-to-medical-devices.pdf.

U.S. Food and Drug Administration (FDA) (2019) General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: U.S. Food and Drug Administration.

U.S. Food and Drug Administration (FDA) (2023a) Cybersecurity in medical devices: Quality system considerations and content of premarket submissions. Silver Spring, MD: U.S. Food and Drug Administration.

U.S. Food and Drug Administration (FDA) (2023b) Content of premarket submissions for management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff. Silver Spring, MD: U.S. Food and Drug Administration.

U.S. Food and Drug Administration (FDA) (2021) Implanted brain-computer interface (BCI) devices for patients with paralysis or amputation: Non-clinical testing and clinical considerations – Guidance for industry and Food and Drug Administration staff. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/implanted-brain-computer-interface-bci-devices-patients-paralysis-or-amputation-non-clinical-testing.

United States Congress (2022) Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, div. FF, title III, § 3305(a), 21 U.S.C. § 360n-2.

U.S. Food and Drug Administration (FDA) (2024) 'Medical devices; Quality System Regulation amendments (Quality Management System Regulation)', Federal Register, 89 FR 7496. https://www.federalregister.gov/documents/2024/02/02/2024-01709/medical-devices-quality-system-regulation-amendments.

U.S. Food and Drug Administration (FDA) (2026a) Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions—Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: U.S. Food and Drug Administration.

U.S. Food and Drug Administration (FDA) (2026b) General Wellness: Policy for Low Risk Devices—Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: U.S. Food and Drug Administration.

UNESCO (2025) New UNESCO report calls for renewed commitment to the right to education. https://www.unesco.org/en/articles/new-unesco-report-calls-renewed-commitment-right-education.

United States Congress (2001) USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 1016(e), 42 U.S.C. § 5195c(e).

Vera, L.A., Walker, D., Murphy, M., Mansfield, B., Siad, L.M., Ogden, J. and EDGI (2019) 'When data justice and environmental justice meet: Formulating a response to extractive logic through environmental data justice', Information, Communication & Society, 22(7), pp. 1012–1028. doi:10.1080/1369118X.2019.1596293.

Vidal, J.J. (1973) 'Toward direct brain-computer communication', Annual Review of Biophysics and Bioengineering, 2(1), pp. 157-180.

Williams, J. (2018) Stand Out of Our Light: Freedom and Resistance in the Attention Economy. Cambridge: Cambridge University Press. doi:10.1017/9781108453004.

Zhang, X. and Wu, D. (2019) 'On the vulnerability of CNN classifiers in EEG-based BCIs', IEEE Transactions on Neural Systems and Rehabilitation Engineering, 27(5), pp. 814–825. doi:10.1109/TNSRE.2019.2908955.

Zhong, S.H., Zhao, S., Xiao, Z., Zhang, Z. and Liu, Y. (2025) 'Attention-guided universal adversarial perturbations for EEG-based brain–computer interfaces', Expert Systems with Applications, 268, p. 126362. doi:10.1016/j.eswa.2024.126362.