From Attack Surface to Psychiatric Diagnosis: A Security Framework for Brain-Computer Interfaces

Anonymous

Abstract

Brain-computer interfaces (BCIs) are transitioning from experimental tools to commercially deployed medical devices. Yet no security framework accounts for the unique risks of devices that read and write neural signals. The Common Vulnerability Scoring System (CVSS v4.0) cannot express biological tissue damage, cognitive integrity violations, or consent boundaries—dimensions critical to neural device security.

We present an integrated framework with four contributions: (1) an 11-band hourglass architecture mapping attack surfaces from neocortex to wireless radio; (2) a threat taxonomy of 102 techniques across 15 tactics and 8 domains; (3) a CVSS v4.0 extension adding five neural-specific metrics; and (4) a methodology mapping security vulnerabilities to DSM-5-TR psychiatric diagnoses.

Analysis reveals that 94.4% of catalogued techniques require neural-specific metrics that CVSS cannot express, and 51 techniques pose direct psychiatric diagnostic risk. We validate the framework through two vulnerability disclosures against real BCI-adjacent systems. The complete framework is released as open source.

1 Introduction

Brain-computer interfaces (BCIs) are no longer confined to research laboratories. Neuralink has implanted its N1 device in human patients [17], Synchron's Stentrode has demonstrated motor neuroprosthesis via neurointerventional surgery [18], and Blackrock Neurotech's Utah array has enabled high-performance speech neuroprostheses [22]. Investment in neurotechnology grew 700% between 2014 and 2021, with the global market projected to reach $25 billion by 2030 [21].

These devices read and write neural signals. An attacker who compromises a BCI does not merely exfiltrate data or disrupt a service—they can induce seizures, decode private thoughts, corrupt memory consolidation, or cause irreversible brain damage. Yet no security framework exists that accounts for these risks.

1.1 The Scoring Gap

The Common Vulnerability Scoring System (CVSS v4.0) [6] is the industry standard for vulnerability assessment. CVSS captures exploitability characteristics and information system impact, but was designed for IT assets. It cannot express:

- **Biological tissue damage**—seizure induction, neural necrosis, involuntary motor activation
- **Cognitive integrity**—thought privacy, perception manipulation, identity modification
- **Consent boundaries**—covert neural manipulation vs. consented therapeutic stimulation
- **Damage reversibility**—IT assets restore from backup; neural tissue cannot be rebooted
- **Neuroplastic consequences**—prolonged adversarial stimulation causes lasting structural brain changes

Our analysis of 102 BCI attack techniques shows that 94.4% require scoring dimensions that CVSS cannot express. When a vulnerability can induce a psychiatric diagnosis, a base score alone is insufficient.

1.2 Contributions

We present an integrated framework with four contributions:

1. **An 11-band hourglass architecture** (Section 3) mapping attack surfaces across neural, interface, and synthetic zones, with a natural security chokepoint at the electrode-tissue boundary.
2. **A threat taxonomy** (Section 4) of 102 techniques across 15 tactics and 8 domains, inspired by the structural methodology of MITRE ATT&CK$^{®}$ and tailored to the BCI domain.
3. **A neural impact scoring extension** (Section 5) for CVSS v4.0, adding five neural-specific metrics and designed to conform with FIRST.org's official extension mechanism [7].

4. **A vulnerability-to-diagnosis pipeline** (Section 6) mapping security vulnerabilities to DSM-5-TR psychiatric diagnoses [1] through a six-stage chain.

We validate the framework through two vulnerability disclosures against real BCI-adjacent systems (Section 7). The complete framework is released as open source.

2 Related Work

Research at the intersection of cybersecurity and neurotechnology has progressed through foundational framing, empirical demonstration, and emerging policy response.

Foundational Neurosecurity. Denning, Kohno, and Chizeck [5, 12] coined "neurosecurity" by analyzing attack surfaces in implantable neurostimulators, identifying wireless reprogramming, battery depletion, and signal injection as threat categories. Bonaci et al. [2] extended this with "App Stores for the Brain," examining privacy threats from third-party BCI applications.

Empirical Attacks. Martinovic et al. [15] demonstrated at USENIX Security 2012 that consumer EEG headsets could be exploited via P300 event-related potentials to extract PINs and personal information through subliminal visual stimuli. This remains the most influential empirical BCI side-channel attack. Wu et al. [23] surveyed adversarial attacks on EEG-based BCIs, documenting adversarial perturbation, backdoor attacks on classifiers, and calibration-phase data poisoning. Halperin et al. [8] established that implanted medical device attacks are practical by demonstrating wireless attacks against pacemakers.

Recent Frameworks. Schroder et al. [20] published the most recent analysis (2025), identifying cyber risks across BCI hardware, software, and communication layers. Ienca and Haselager [10] analyzed BCI security through informational and physical integrity, proposing that BCIs require both cybersecurity and neuroethical safeguards. Camara et al. [3] and Rushanan et al. [19] surveyed security in implantable medical devices broadly, covering pacemakers and neurostimulators.

Neuroethics and Policy. Ienca and Andorno [9] proposed four neurorights (cognitive liberty, mental privacy, mental integrity, psychological continuity). UNESCO's 2025 Recommendation [21], adopted by 194 Member States, is the first global normative framework for neurotechnology governance.

Gap. Prior work addresses BCI security, neuroethics, and vulnerability scoring separately. No existing framework integrates architecture, technique-level taxonomy, CVSS-compatible scoring, and clinical impact mapping into a single system. The vulnerability-to-diagnosis pipeline has no precedent in either cybersecurity or neuroethics literature.

3 The Hourglass Architecture

The proposed architecture maps the full BCI attack surface using an 11-band hourglass model organized into three zones. The model derives from two independent design traditions: the OSI networking reference model [24], which stratifies communication systems into functional layers, and functional neuroanatomy [11], which organizes the nervous system by structure and physiological role. The hourglass shape borrows from the Internet protocol architecture [4], where IP serves as a narrow waist through which all traffic must pass.

3.1 Design Rationale

A BCI system spans from cortical computation to radio transmission. The neural interface—the electrode-tissue boundary—forms a natural chokepoint analogous to IP: all signals must cross this boundary. Above it, attack surfaces expand through the complexity of neural tissue. Below it, they expand through electronic and wireless systems. The resulting shape is an asymmetric hourglass.

3.2 Band Definitions

The model uses a 7-1-3 structure: seven neural bands (N7–N1) corresponding to the canonical CNS hierarchy [11], one interface band (I0), and three synthetic bands (S1–S3).

Table 1: Hourglass architecture: 11 bands across three zones.

Band	Name	Zone	Attack Surface
N7	Neocortex	Neural	Executive function, language, movement
N6	Limbic System	Neural	Emotion, memory, interoception
N5	Basal Ganglia	Neural	Motor selection, reward, habit
N4	Diencephalon	Neural	Sensory gating, consciousness relay
N3	Cerebellum	Neural	Motor coordination, timing
N2	Brainstem	Neural	Vital functions, arousal, reflexes
N1	Spinal Cord	Neural	Reflexes, peripheral relay
I0	Neural Interface	Interface	Electrode-tissue boundary
S1	Analog	Synthetic	Amplification, ADC, near-field EM
S2	Digital	Synthetic	Decoding, BLE/WiFi, telemetry
S3	Radio	Synthetic	RF, directed energy, app layer

3.3 Security Properties

The architecture provides three properties: (1) *completeness*—every BCI component maps to exactly one band;

(2) *chokepoint identification*—I0 is the natural monitoring point for all bio-digital signal transit; and (3) *threat locality*—each technique in the taxonomy is annotated with affected bands, enabling defenders to understand the spatial extent of an attack.

Ascending the neural hierarchy, attacks produce qualitatively different harms: N1–N2 attacks threaten vital functions (respiratory arrest, cardiac dysregulation); N5–N7 attacks threaten cognition, identity, and autonomy. This *determinacy gradient* has direct security implications: lower-band attacks are more predictable and immediately dangerous, while higher-band attacks are less predictable but potentially more insidious.

4 Threat Taxonomy

We catalog 102 BCI attack techniques with a structure inspired by MITRE ATT&CK [16], independently developed to cover neural, cognitive, and physical safety domains. Each technique is simultaneously an attack vector, an ethical risk, and—where applicable—a therapeutic application.

Why not ATT&CK directly? MITRE ATT&CK is designed for enterprise IT. BCI threats differ fundamentally: (1) the target is biological tissue, not an information system—attacks can cause seizures or cognitive coercion; (2) the same technique is often simultaneously an attack and a therapy (e.g., deep brain stimulation); and (3) the attack lifecycle crosses the bio-digital boundary that ATT&CK's purely digital model does not address.

4.1 Structure

The taxonomy organizes 102 techniques into 15 tactics across 8 domains spanning the full attack lifecycle: Neural (N), BCI System (B), Protocol (P), Data (D), Cognitive (C), Countermeasure (M), Evasion (E), and Sensor (S).

4.2 Evidence and Severity

Each technique carries an evidence status: Confirmed (19), Demonstrated (33), Emerging (22), Theoretical (26), Plausible (1), Speculative (1). CVSS v4.0 base severity is heavily weighted toward high and critical: 29 critical (28.4%), 54 high (52.9%), 16 medium (15.7%), 3 low (2.9%).

4.3 Dual-Use Mapping

A distinctive feature is systematic dual-use mapping: every technique is assessed for therapeutic analogs. The same mechanisms that enable attacks—electromagnetic stimulation, signal decoding, neuromodulation—underlie established therapies (DBS [14], TMS [13], neurofeedback).

Table 2: Dual-use classification of 102 techniques.

Class	Definition	Count	%
Confirmed	Published clinical use	52	51.0%
Probable	Under clinical investigation	16	15.7%
Possible	Theoretical therapeutic map	9	8.8%
Silicon Only	No tissue analog	25	24.5%

Of the 102 techniques, 77 (75.5%) have confirmed or probable therapeutic analogs. The boundary between attack and therapy is not mechanism—it is consent, dosage, and oversight.

4.4 Representative Techniques

Table 3: Five representative techniques.

Sev.	Status	Dual-Use	Description
Critical	Confirmed	Confirmed	Cortical signal injection via rogue electrode stimulation
High	Demonstrated	Confirmed	P300 side-channel extraction of private information [15]
High	Emerging	Probable	Calibration data poisoning during BCI training sessions
Medium	Confirmed	Confirmed	Ultrasonic side-channel via bone conduction
High	Demonstrated	Confirmed	WiFi CSI passive body sensing for respiratory inference

5 Neural Impact Scoring

We propose a CVSS v4.0 extension designed to conform with FIRST.org's official extension mechanism (User Guide §3.11) [7]. The extension adds five metrics capturing dimensions CVSS cannot express.

5.1 Gap Analysis

Mapping all 102 techniques to CVSS v4.0 base vectors reveals three gap groups:

Table 4: CVSS v4.0 gap analysis.

Group	Gap Description	Count
1	CVSS captures most impact; extension adds nuance	12
2	CVSS captures exploitability but misses half	28
3	CVSS fundamentally cannot express primary impact	58
	Techniques needing extension	**98 (96.1%)**

5.2 Extension Metrics

Five metrics, each orthogonal to CVSS base metrics:

Biological Impact (BI). Direct harm to neural tissue or physiological function. Values: None (0.0), Low (3.3, temporary discomfort), High (6.7, seizure induction, involuntary motor activation), Critical (10.0, life-threatening or permanently disabling).

Cognitive Integrity (CG). Impact on thought processes, perception, memory, or identity. Values: None (0.0), Low (3.3, partial intent exposure), High (6.7, full thought decoding or perception manipulation), Critical (10.0, cognitive coercion or identity modification).

Consent Violation (CV). Degree of informed consent violation. Values: None (0.0), Partial (3.3, scope exceeded but subject aware), Explicit (6.7, direct violation, detectable), Implicit (10.0, covert manipulation the patient cannot detect).

Reversibility (RV). Whether damage can be undone. Values: Full (0.0, effects cease with attack), Temporary (3.3, hours to days), Partial (6.7, some permanent), Irreversible (10.0, permanent neural destruction).

Neuroplasticity (NP). Whether the attack exploits or induces neuroplastic changes. Values: None (0.0), Temporary (5.0, short-term synaptic), Structural (10.0, long-term pathway changes).

5.3 PINS Flag

The Potential Impact to Neural Safety (PINS) flag triggers when BI $\geq$ High or RV = Irreversible, mandating immediate safety review. 31 of 102 techniques (30.4%) are PINS-flagged.

5.4 Dual-Vector Architecture

The extension vector rides alongside CVSS:

```
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
NISS:1.0/BI:H/CG:C/CV:I/RV:P/NP:S
```

Security teams triage using familiar CVSS scores while BCI-specific teams see the neural dimensions that determine whether a vulnerability is a software bug or a patient safety emergency.

6 From Vulnerability to Diagnosis

We introduce a six-stage pipeline for mapping security vulnerabilities to clinical psychiatric diagnoses. To our knowledge, this is the first systematic methodology connecting cybersecurity severity to DSM-5-TR diagnostic codes [1].

6.1 Pipeline

Each technique is traced through six stages: (1) **Technique**: the attack; (2) **Band**: which hourglass band(s) it affects; (3) **Neural structure**: the anatomy at risk; (4) **Cognitive function**: what that structure supports; (5) **Neural impact score**: particularly the BI, CG, and NP metrics; (6) **DSM-5-TR code**: the psychiatric diagnosis associated with disruption of that function.

The bridge from scoring metrics to diagnostic clusters is driven by which metric dominates: BI-driven techniques map to motor/neurocognitive disorders; CG-driven to cognitive/psychotic clusters; CV-driven to mood/trauma disorders; NP/RV-driven to persistent personality changes.

6.2 Coverage

All 102 techniques have been mapped:

Table 5: Impact chain mapping results.

Metric	Value
Techniques mapped	102 / 102
Unique DSM-5-TR codes	15
Diagnostic clusters	5
Direct diagnostic risk	51 (50.0%)
Indirect diagnostic risk	9 (8.8%)
No diagnostic risk	42 (41.2%)

The five clusters are: Non-diagnostic (42), Mood/Trauma (21, e.g., F43.10 PTSD, F32.9 MDD), Cognitive/Psychotic (16, e.g., F06.0 psychosis), Motor/Neurocognitive (16, e.g., G25.9 movement disorder), and Persistent/Personality (7, e.g., F07.0 personality change).

6.3 Example: Cortical Signal Injection

Tracing one technique through the full chain:

1. **Technique**: Cortical signal injection
2. **Band**: N7 (Neocortex), N6 (Limbic)
3. **Structure**: Motor cortex (M1), prefrontal cortex, hippocampus
4. **Function**: Motor control, executive function, memory
5. **Score**: BI:C/CG:H/CV:I/RV:P/NP:S $\rightarrow$ 8.7 (High), PINS flagged

6. **DSM-5-TR**: G25.9 (movement disorder), F06.0 (psychosis due to medical condition), F07.0 (personality change)
7. **Risk**: Direct—stimulation itself triggers seizures, involuntary movement, perception distortion

A CVSS score of 9.3 tells a security team this vulnerability is critical. The impact chain tells a clinical team it can cause a movement disorder, psychosis, and personality change. Both are needed.

7 Case Studies

We validate the framework through two channels: scoring comparisons that demonstrate the gap between CVSS-only and extended scoring, and real vulnerability disclosures against BCI-adjacent systems.

Caveat: Cases 1–4 are threat model scenarios derived from the taxonomy. They represent plausible attacks based on known neuroscience and engineering but have not been executed against real BCI hardware. Case 5 involves an empirically confirmed vulnerability.

7.1 Scoring Comparison

Table 6: CVSS v4.0 vs. neural-extended scoring.

Technique	**CVSS**	**Extension**
Cortical signal injection	9.3 (Crit)	8.7 (High)
P300 side-channel [15]	7.7 (High)	4.7 (Med)
Calibration poisoning	8.2 (High)	5.3 (Med)
Covert neural surveillance	7.1 (High)	6.0 (Med)
Ultrasonic bone-conduction	5.3 (Med)	2.7 (Low)

The key observation: CVSS and the extension do not always agree on severity ranking. Cortical signal injection scores high on both because it is both exploitable *and* biologically devastating. P300 side-channel scores high on CVSS (confidentiality breach) but medium on the extension (no physical harm—the attack is passive). This distinction matters for clinical triage.

7.2 Case 5: BCI Streaming Library Vulnerability

During systematic analysis of the BCI software ecosystem, we identified a multi-phase exploit chain in a widely-used open-source library for neural data streaming. The library is deployed in clinical and research BCI pipelines across multiple institutions.

The exploit chain demonstrates escalation from synthetic-zone vulnerabilities (S2/S3 bands) to potential neural-zone impact: corrupted data reaching clinical decision-making systems. CVSS scores the software vulnerabilities accurately; the neural extension captures downstream risk to patients whose care depends on data stream integrity.

Responsible disclosure was initiated prior to this submission. The vulnerability was reported to maintainers on February 11, 2026. Specific details—including affected software, CWE identifiers, and proof-of-concept—will be published after coordinated disclosure concludes.

A second vulnerability—a 9-year-old flaw in a widely-deployed audio codec used in neural signal processing pipelines—was filed through a national CERT coordination center. CVE assignment is pending.

8 Ethics

Beneficence. This work presents the first integrated security framework for brain-computer interfaces, enabling manufacturers, regulators, and researchers to assess neural-specific risks. The threat taxonomy could theoretically inform attackers; however, all 102 techniques are derived from published literature or established therapeutic protocols. No novel attack code is disclosed. 75.5% of catalogued techniques have confirmed or probable therapeutic analogs—the knowledge is already in clinical use.

Respect for persons. No human subjects were involved. No BCI devices were tested on patients. All vulnerability research was conducted on software systems, not devices in clinical use.

Justice. The complete framework is released under the Apache 2.0 license. It is designed to protect vulnerable populations—BCI patients with paralysis, locked-in syndrome, and epilepsy—who cannot opt out of their devices.

Responsible disclosure. *Vulnerability 1* (BCI data streaming library): Disclosed to maintainers on February 11, 2026, prior to this submission. We are awaiting establishment of a private disclosure channel. No exploit code has been published. Full proof-of-concept is withheld pending vendor patch. *Vulnerability 2* (audio codec): Filed through a national CERT coordination center. CVE assignment is pending.

Both disclosures follow coordinated vulnerability disclosure best practices. This paper does not contain sufficient detail to reproduce either exploit.

9 Limitations and Future Work

We present these limitations transparently.

No empirical validation on BCI hardware. The taxonomy was developed through literature review and threat modeling, not penetration testing of neural devices. Only the synthetic zone has been validated against real software (Section 7).

DSM-5-TR mapping not clinically validated. The impact chain mappings have not been reviewed by psychiatrists or clinical neuroscientists. They represent our best assessment based on neuroanatomical pathways and functional neuroscience.

Scoring weights not calibrated. The extension uses equal weights for all five metrics. Context profiles (clinical, research, consumer, military) propose differential weights but lack empirical calibration.

No interrater reliability. Scores were assigned by a single analyst. A formal interrater reliability study with domain experts from both cybersecurity and neuroscience is needed.

Single-author bias. The framework was developed by a single independent researcher. Multi-model AI verification was used throughout development; architectural decisions and scoring assignments reflect a single perspective. Peer review is essential for maturation.

Future work. (1) Clinical validation with psychiatrists; (2) interrater reliability study; (3) formal registration of the scoring extension with FIRST.org; (4) penetration testing against BCI hardware; (5) weight calibration via expert elicitation.

10 Conclusion

Brain-computer interfaces are transitioning from laboratory prototypes to commercial medical devices. A vulnerability in a BCI is not merely a software bug—it is a potential path to seizures, cognitive manipulation, thought-level privacy violation, and irreversible neural harm.

We presented an integrated framework comprising an 11-band architecture, a 102-technique threat taxonomy, a CVSS v4.0 extension with five neural-specific metrics, and a first-of-its-kind pipeline mapping security vulnerabilities to DSM-5-TR psychiatric diagnoses. Analysis reveals that 94.4% of techniques require scoring dimensions CVSS cannot express, 75.5% have therapeutic dual-use analogs, and 58.8% pose direct or indirect psychiatric diagnostic risk. We validated the framework through two vulnerability disclosures against real BCI-adjacent systems.

The framework has significant limitations—documented transparently in Section 9. These are invitations to collaborate, not reasons to delay. The BCI industry is moving faster than security standards. The question is not whether neural security frameworks are needed. The question is whether they will be ready before the first patient is harmed.

Availability

The complete framework, threat registry, and scoring system are released as open source under the Apache 2.0 license.[1] An interactive threat registry browser and scoring calculator are available at the project website.

References

[1] American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR)*. American Psychiatric Association Publishing, 2022.

[2] Tamara Bonaci, Ryan Calo, and Howard J. Chizeck. App stores for the brain: Privacy & security in brain-computer interfaces. *IEEE Technology and Society Magazine*, 34(2):32–39, 2015.

[3] Carmen Camara, Pedro Peris-Lopez, and Juan E. Tapiador. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, 55:272–289, 2015.

[4] Stephen Deering. Watching the waist of the protocol hourglass. 2001. Foundational description of the Internet hourglass architecture.

[5] Tamara Denning, Yoky Matsuoka, and Tadayoshi Kohno. Neurostimulators in security-sensitive applications: Exploring the neurosecurity design space. In *Proceedings of the USENIX Workshop on Health Security and Privacy*, 2009.

[6] FIRST.org. Common vulnerability scoring system v4.0 specification, 2023.

[7] FIRST.org. CVSS v4.0 user guide, 2023. Section 3.11: Extension Framework.

[8] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, pages 129–142, 2008.

[9] Marcello Ienca and Roberto Andorno. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy*, 13(1):5, 2017.

[1] Repository URL withheld for double-blind review.

[10] Marcello Ienca and Pim Haselager. Hacking the brain: Brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, 18(2):117–129, 2016.

[11] Eric R. Kandel, John D. Koester, Sarah H. Mack, and Steven A. Siegelbaum. *Principles of Neural Science*. McGraw-Hill, 6th edition, 2021.

[12] Tadayoshi Kohno, Tamara Denning, and Howard J. Chizeck. Neurosecurity: Security and privacy for neural devices. In *Neurosurgical Focus*, 2009. First use of the term "neurosecurity" in academic literature.

[13] Joachim K. Krauss, Nir Lipsman, Tipu Aziz, et al. Technology of deep brain stimulation: Current status and future directions. *Nature Reviews Neurology*, 17:75–87, 2021.

[14] Andres M. Lozano, Nir Lipsman, Hagai Bergman, et al. Deep brain stimulation: Current challenges and future directions. *Nature Reviews Neurology*, 15:148–160, 2019.

[15] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the 21st USENIX Security Symposium*, pages 143–158. USENIX Association, 2012.

[16] MITRE Corporation. ATT&CK® framework, 2024.

[17] Elon Musk and Neuralink. An integrated brain-machine interface platform with thousands of channels. *Journal of Medical Internet Research*, 21(10):e16194, 2019.

[18] Thomas J. Oxley, Peter E. Yoo, Gill S. Rind, et al. Motor neuroprosthesis implanted with neurointerventional surgery improves capacity for activities of daily living tasks in severe paralysis. *Journal of NeuroInterventional Surgery*, 13:102–108, 2021.

[19] Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, and Colleen M. Swanson. SoK: Security and privacy in implantable medical devices and body area networks. pages 524–539, 2014.

[20] Tyler Schroder, Shyam Sunder Bhatt, and Sandeep Bhatt. Cyber risks to next-generation brain-computer interfaces: Analysis and recommendations. *arXiv preprint arXiv:2501.09566*, 2025.

[21] UNESCO. Recommendation on the ethics of neurotechnology. Adopted at the 43rd session of the General Conference, Samarkand, 2025.

[22] Francis R. Willett, Erin M. Kunz, Chaofei Fan, et al. A high-performance speech neuroprosthesis. *Nature*, 620:1031–1036, 2023.

[23] Zitong Wu, Guoyu Yao, Xiang Zhang, and Zhilin Li. Adversarial attacks on EEG-based brain-computer interfaces: A comprehensive survey. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 2024.

[24] Hubert Zimmermann. OSI reference model — the ISO model of architecture for open systems interconnection. *IEEE Transactions on Communications*, 28(4):425–432, 1980.