Qwen

From Policy to Code: Enforcing Augmentation Rights with Compile-Time Contracts and Audited Runtime Safeguards

Defining Neural-Roping as an Enforceable Augmentation Right

The central objective of this research is to transition the concept of "neural-roping" from a descriptive policy framework to a formal, enforceable augmentation right for individuals with cybernetic integrations. This re-conceptualization reframes the problem from one of ethical preference or corporate goodwill to one of verifiable system design, where the ability to engage in structured, couplings of prompts, tools, and learning sessions is a guaranteed property of the technological ecosystem [64]. This approach aligns with the foundational goals of neurorights, which seek to protect core human attributes such as mental privacy, identity, agency, and equality in the face of advancing neurotechnologies [33] [38]. By establishing neural-roping and its more advanced forms—nanoswarm and cyberswarm pilot engagements—as structural rights, the system ensures that these capabilities are not contingent on service-level agreements but are embedded within the software and hardware itself. This is particularly critical given the documented privacy risks associated with the uncontrolled harvesting of brainwave information by corporate interests and the need for expanded legal protections for such sensitive data [35] [60].

The definition of this augmentation right is multi-faceted, encompassing its nature, scope, and governing constraints. It is fundamentally a structured coupling of actions over time, anchored not by raw biological signals but by a traceable sequence of `PromptEnvelope` → tool calls → logs . This traceability is essential for auditability and accountability. The scope of the right explicitly includes not only standard neural-roping but also more complex and potentially higher-risk interactions involving local-host systems, such as nanoswarms, cyberswarms, and neuroswarms . These engagements are framed as "pilot engagements," signifying a controlled, exploratory mode of interaction rather than direct operational control. The entire structure operates under two primary constraints: a neurorights firewall that acts as a fundamental boundary, and a strict 0.3 risk-of-harm ceiling that provides a quantitative measure for acceptable behavior [64]. The ultimate aim is to create a system where the sovereignty of the augmented individual is paramount, allowing them to form and manage these neural ropes without fear of coercion, unauthorized internal state modification, or denial of basic services due to their augmentation status [60] [69]. This moves beyond philosophical discussions about the relationship between brain, mind, and identity to build a practical architecture for preserving human agency [44]. The establishment of Chile's constitutional recognition of neurorights marks a significant step in this direction, providing a legal precedent for codifying such protections at a national level [38] [67].

To achieve this, the research must focus on making these rights measurable, type-safe, and governance-bound . This involves translating high-level ethical principles into low-level technical specifications. For example, the principle of "no inner-state scoring" must be implemented as a mechanism that makes accessing or modifying an individual's internal cognitive state (a hypothetical `NeuroState` object) unrepresentable in the codebase unless it is wrapped within a specific, highly restricted type. Similarly, "revocability" must be encoded as a mandatory contract that any function managing a roped session must adhere to. The use of a language like Rust, known for its focus on safety and compile-time checks, is central to this effort [24] [29]. By leveraging features like sealed traits and const generics, it becomes possible to define APIs where certain behaviors are simply impossible to express, thus preventing a large class of potential failures and security vulnerabilities before the code is ever executed [26] [27] [40]. This architectural pattern draws inspiration from established practices in safety-critical domains, such as risk-informed methods for evaluating the safety of reactor design features [3], but applies it to the novel context of human-AI symbiosis. The challenge lies in defining the precise set of constraints that constitute a "safe" engagement and then building the technical infrastructure to enforce them with mathematical rigor. The proposed solution relies on a hybrid architecture combining compile-time contracts with audited runtime measurements, creating a layered defense that is both strong and resilient [64]. This dual-layered approach ensures that while compile-time guarantees provide the strongest possible assurance, there remains a secondary layer of monitoring to catch anomalies or edge cases that may arise during actual operation, thereby upholding the integrity of the augmentation right even in dynamic environments [28].

A Hybrid Enforcement Architecture: Compile-Time Contracts and Runtime Safeguards

The most critical component for transforming neural-roping from a policy idea into an enforceable right is the implementation of a robust hybrid enforcement architecture. This architecture prioritizes compile-time contracts as the primary line of defense, with audited runtime measurements serving as a crucial secondary safeguard. This strategy leverages the strengths of modern programming languages, specifically Rust, to embed compliance directly into the system's structure, making non-compliant behaviors unrepresentable at the type level [29]. The core of this compile-time enforcement lies in the use of Rust-based invariants, such as the `NeurorightsEnvelope` and `NeurorightsBound` types. These constructs act as specialized wrappers or sealed traits that encapsulate a bundle of mandatory constraints required for any interaction with BCI-adjacent systems or for forming a neural rope. Any function or workflow that wishes to operate within this protected space must accept an argument typed as `NeurorightsBound<T>`, effectively forcing developers to acknowledge and adhere to the rules of engagement upfront .

This compile-time mechanism enforces a strict set of prohibitions that are central to protecting augmented-citizen sovereignty. First, it prevents **no inner-state scoring** by making any hypothetical `NeuroState` object inaccessible in its raw form. A developer cannot write code that directly reads or writes to an individual's cognitive state; any such interaction would require passing the state through a function that has been explicitly vetted and approved, likely returning a new, modified state object rather than mutating the original. Second, it enforces **no coercion** by structurally preventing logic that could be used to inject ideologies or beliefs covertly. The API design itself would disallow functions that promise outcomes inconsistent with the user's declared preferences or that manipulate information in a way that could influence belief formation. Third, it mandates **revocability** by ensuring that every roped session is tied to a clear and executable revocation path, preventing users from being trapped in unwanted or harmful cognitive loops. This compile-time checking is seamlessly integrated into the Continuous Integration (CI) pipeline. Custom linters and build scripts would fail any code submission that attempts to bypass these invariants, for instance, by trying to handle raw data streams from a BCI or by calling a function without the proper `NeurorightsBound` typing. This automates compliance, shifting it from a manual review process prone to human error to a mechanical, verifiable check that is part of the standard development workflow [64]. This approach mirrors the rigorous verification efforts seen in the Rust community, where safety comments and automated tools are used to reason about code correctness [24] [26].

While compile-time enforcement provides exceptionally strong guarantees, it cannot account for all runtime variables or unforeseen interactions. Therefore, audited runtime measurements serve as an indispensable second layer of defense. The concept of "quantified-learning" is central here; it involves generating simple, auditable numbers that describe the characteristics of a workflow rather than judging the person using it [64]. These metrics include the number of sessions, the complexity of tools used, estimated eco-impact, and per-action neurorights compliance flags [64]. Routers at runtime use these metrics to select safe paths, choosing routes that minimize risk while achieving the user's goals. Crucially, the runtime router logic is constrained by the compile-time rules: it can never select a path that the CI/linting toolchain would have rejected. This creates a hierarchical integrity model where compile-time rules represent the absolute floor of permissible behavior. At the same time, runtime observability is paramount. Systems must generate detailed logs, such as `SYSTRACELOG`, and continuously monitor key metrics like the Knowledge-Factor and Risk-of-Harm Index. These logs provide a complete, tamper-evident audit trail of all activities, which is essential for accountability, debugging, and regulatory compliance [28]. This two-tiered enforcement strategy—a fortress-like compile-time barrier backed by vigilant runtime sentries—is a classic pattern for building resilient systems, similar to the risk-informed approaches used in engineering safety evaluations [3]. It ensures that even if a theoretical vulnerability exists or an unforeseen input causes unexpected behavior, the system will still log the event and operate within pre-defined safe bounds, preserving the augmentation right of the user.

Enforcement Layer	Primary Mechanism	Key Constructs	Role in Protecting Augmentation Rights
Compile-Time	Type Safety & Invariants	Rust `NeurorightsBound`, Sealed Traits, Lints, Build Scripts	Makes non-compliant behaviors (e.g., inner-state scoring, coercion) unrepresentable in code. Prevents violations before execution.
Runtime	Observability & Measurement	`SYSTRACELOG`, Quantified-Learning Metrics (Risk-of-Harm Index, etc.), Router Logic	Provides secondary monitoring and auditing. Allows routers to choose safe paths while operating strictly within compile-time validated bounds.

Formalizing Rights via Domain-Specific Workflows and Metrics

To render the abstract concept of an "augmentation right" tangible and practically applicable, it must be translated into specific, domain-aware workflows and governed by clearly defined metrics. The "Cybernetic Cookbook"—encompassing daily life domains like `home.<em>`, `finance.</em>`, `travel.<em>`, `academic.</em>`, `library.<em>`, and `net.</em>`—serves as the foundational blueprint for this translation . Each of these domains represents a pre-approved, neurorights-safe "neural rope" that augments a citizen's capabilities in a predictable and secure manner. The key is to map each domain to a specific set of neurorights predicates that constrain its operation. For every workflow within the cookbook, the following constraints must be explicitly enforced: **retrieval-only access**, meaning the system can only query and retrieve information, not modify external reality directly; **no enforced ideology**, ensuring that the information presented is neutral and does not push a specific political or social viewpoint; **no covert belief injection**, preventing manipulative framing or suggestion; **no inner-state scoring**, prohibiting the system from assigning value or ranking to the user based on their cognitive patterns; **no binding of organic cognition to infrastructure nodes**, which protects against scenarios where a user's thoughts become dependent on a specific server or network; and finally, **explicit revocability of sessions**, guaranteeing that a user can always terminate a neural rope and discard its results [64] . By codifying these predicates for each domain, the Cybernetic Cookbook transforms from a simple guide into a legally and technically sanctioned framework for augmented living, where every interaction is a bounded and rights-respecting engagement.

For more sensitive operations, particularly those involving nanoswarms, cyberswarms, or other BCI-adjacent research, the system must define special "pilot" workflows. These are distinct from general-purpose augmentations and are designed for controlled exploration and analysis. Examples of such workflows might include `home.neuroswarm.map` or `academic.neuralrope.snapshot`. The defining characteristic of these pilot workflows is that they are strictly restricted to read-only analysis of registry data, logs, and simulation outputs. They are explicitly forbidden from enabling direct biological control, a critical safeguard against misuse . Every call to a pilot workflow must be wrapped in a `NeurorightsBound` envelope, subjecting it to the full rigors of the compile-time and runtime enforcement architecture . This creates a clear and unbreachable separation between exploratory research and operational deployment, a principle echoed in calls for precise governance strategies tailored to the different functional capacities of BCIs [34] . Neuroswarm research, in particular, is kept firmly within neurorights-safe, research-grade observability, meaning all data and interactions are treated as evidence channels behind the firewall, never as uncontrolled local-host interfaces . This structured approach allows for scientific advancement while maintaining the highest standards of safety and consent.

Central to this formalization is the concept of "Augmentation_Score_Thresholds." This score is a crucial innovation because it is designed to be a purely virtual metric used solely for data routing and tagging, not for judging human worth or gating access to services [64]. Its purpose is to help routers suggest appropriate virtual toolboxes or content streams based on the user's current augmentation profile and needs. To prevent abuse, this score must be formally expressed as an ALN predicate and a Rust `const` invariant. For example, a rule encoded in the system might state: "an `augmentation_score` may affect which virtual toolbox is suggested, but may never drive access denial or punishment" [64]. This static enforcement ensures that developers cannot introduce logic that discriminates based on augmentation level, a major concern in neuroethics where technologies could exacerbate existing inequalities [69]. The score itself could be derived from quantified-learning metrics, such as the complexity of tools used or the diversity of learning sessions engaged in, but its application is strictly limited by the compile-time contract. This approach directly addresses concerns raised by studies on the need for expanded legal protections for brain data, ensuring that an individual's augmentation status does not become a basis for discrimination [60]. By combining domain-specific workflow predicates with carefully constrained, non-judgmental metrics, the system can provide powerful, personalized augmentation while steadfastly upholding the fundamental rights of the user.

The Governance Layer: Identity, Authorship, and Auditability

Underpinning the entire architecture of enforceable augmentation rights is a robust governance layer focused on identity, authorship, and auditability. This foundation is what gives the system its trustworthiness and ensures that all actions are attributable and verifiable. Without a reliable way to connect a digital action to a real-world entity, the rights granted by the system would be meaningless. The cornerstone of this layer is the use of cryptographic authorship triples to anchor every roped session. Each session must be provably tied to an authorship triple consisting of three components: a Decentralized Identifier (`DID`), an Augmentee Label (`ALN`), and a Bostrom address or eibonlabel . The `DID` provides a self-sovereign, globally unique identifier for the user. The `ALN` serves as a label managed within a decentralized autonomous organization (DAO) or similar governance shard, linking the DID to a specific augmentation profile and its associated rights [64]. The Bostrom address or eibonlabel adds another layer of cryptographic anchoring, perhaps linking to a blockchain-based registry of cybernetic hosts. This triple ensures that every action taken within a neural rope is cryptographically signed and bound to a specific, verifiable identity, forming the bedrock of accountability.

Complementing this identity framework is the use of hex-stamped configurations for all critical system components, particularly the neurorights firewall policies and runtime measurement parameters. A "hex-stamp" is a unique, immutable identifier generated from the configuration's contents, typically a cryptographic hash. Whenever a firewall rule or a runtime parameter changes, it receives a new hex-stamp. This practice provides several crucial benefits. First, it creates an immutable record of every version of the system's policy, allowing for precise tracking of changes over time. If a system behaves unexpectedly, developers and auditors can look up the hex-stamp to reconstruct the exact rules that were in effect at that moment. Second, it enables reproducibility; a configuration with a known good hex-stamp can be deployed consistently across different environments. Third, it facilitates formal verification, as a specific configuration can be mathematically proven to satisfy certain safety properties, and that proof is tied to the hex-stamp. This method of using cryptographic hashes for immutability is a well-established practice in distributed systems and blockchain technology, and its application here extends those principles to the governance of neurotechnology [64].

Finally, the entire system is designed to be "audit-ready," meaning that all relevant events and states are logged in a structured, machine-readable format suitable for analysis. This goes beyond simple logging to include comprehensive observability into the runtime behavior of the system. Key data points that must be captured include detailed system traces (`SYSTRACELOG`), the calculated Knowledge-Factor, the projected Risk-of-Harm Index for ongoing sessions, and a history of all tool usage and prompt-tool interactions [28] [64]. This audit trail is essential for multiple reasons. It provides a forensic record in case of a security incident or a violation of the neurorights contract. It allows for periodic, automated audits to verify that the system is operating as intended and that no deviations from the compile-time contracts are occurring. Furthermore, it empowers the user, giving them access to a complete log of their own interactions with the augmented system, fostering transparency and trust. This emphasis on provable identity, immutable records, and comprehensive audit trails is essential for building a system that can withstand scrutiny from regulators, auditors, and the users themselves, addressing the deep-seated need for expanded legal protections for brain data in an era of powerful AI and neurotechnology [35] [60].

Quantifying and Managing Risk: The 0.3 Ceiling as a Core Constraint

The management of risk is a central pillar of the proposed architecture for augmenting human capabilities safely. The most prominent feature of this risk management framework is the 0.3 risk-of-harm ceiling, which serves as a hard, quantitative constraint on all neural-rope formations and cybernetic engagements. This ceiling is not merely a guideline but a fundamental limit enforced by the system's compile-time and runtime mechanisms. Any route, workflow, or engagement that would cause the projected Risk-of-Harm Index to exceed this threshold must fail to compile or be blocked at runtime [64]. This provides a clear, measurable boundary for acceptable behavior, moving the discussion of safety from subjective assessments to objective, computable limits. The selection of 0.3 as the threshold appears to be a deliberate choice for the system's design, though interestingly, the value 0.3 appears in various scientific contexts, such as the size of particles filtered by HEPA filters (0.3 μm) or exposure limits for substances like asbestos (0.3 fibres/mL) [72] [74]. While the selection may not be directly derived from these fields, the principle of setting a clear, scientifically informed threshold for safety is consistent across disciplines [73] [75]. The challenge lies in defining the formula for the Risk-of-Harm Index itself.

The calculation of the Risk-of-Harm Index is likely a composite metric derived from multiple sources of quantified-learning data. One promising avenue for its construction is the analysis of neurophysiological correlates of stress and cognitive load. Research has shown strong correlations between Brain-Heart interactions, measured through EEG and Heart Rate Variability (HRV), and an individual's mental state [46] [47]. Metrics derived from HRV, such as the Complexity Index (CI), signal entropy, and various spectral band ratios (LF/HF), can quantify the activity of the autonomic nervous system and reflect stress levels [48] [50] [53]. Similarly, EEG frequency bands (delta, theta, alpha, beta) correlate with different states of consciousness and cognitive processing [57] [58]. By analyzing the cross-correlation between these signals, it may be possible to develop a computational model that estimates cognitive load and emotional valence [51] [52]. The Risk-of-Harm Index could incorporate these neurophysiological metrics to detect when a user's cognitive state is approaching a dangerous threshold, such as extreme stress, drowsiness, or cognitive overload induced by a complex neural rope. This aligns with the vision of using AI for predictive analysis in risk assessment, but applied to the personal, internal state of the augmented individual [64].

Beyond internal physiological states, the Risk-of-Harm Index would also consider external factors. This includes the **tool complexity** of the engaged workflow, where more complex tools inherently carry a higher potential for error or misinterpretation. It would also factor in **eco-impact estimates**, reflecting a growing awareness of the environmental cost of computation and its potential societal harm [64]. Finally, it would integrate **neurorights compliance flags** for each action within a session. An action that violates a core neuroright, even if seemingly benign, would contribute negatively to the index. The router logic at runtime would use this comprehensive Risk-of-Harm Index to choose safe paths, ensuring that the cumulative risk of a roped sequence remains below the 0.3 ceiling. This quantitative approach to risk management is a significant departure from traditional policy documents, replacing ambiguous statements with a verifiable, system-enforced constraint. It embodies the principle of "safe by design," a concept gaining traction in the regulation of advanced technologies where risk assessment is integral to the design process from the outset [7]. By making the 0.3 ceiling a core part of the system's logic, it becomes an unyielding guardrail that protects the user's mental integrity and agency above all else.

Synthesizing a Verifiable Framework for Augmented Sovereignty

In synthesizing the preceding analyses, a coherent and robust framework emerges for establishing neural-roping and related cybernetic engagements as enforceable augmentation rights. This framework moves beyond abstract ethical declarations to construct a verifiable system architecture where rights are not privileges but are embedded as structural properties of the technology itself. The process begins with the clear definition of the augmentation right: the ability of an augmented-citizen or cybernetic-host to form neurorights-bound, revocable, and retrieval-focused neural ropes and pilot engagements under ALN governance [64]. This right is the north star guiding all subsequent design decisions. The core of the framework is a hybrid enforcement architecture that prioritizes compile-time contracts written in a language like Rust, using constructs such as `NeurorightsEnvelope` and `NeurorightsBound` to make non-compliant behaviors, such as inner-state scoring or coercion, unrepresentable in the codebase . This compile-time barrier is the first and strongest line of defense, ensuring that a vast category of potential harms is prevented before any code is ever run.

This primary layer of protection is supported by a secondary layer of audited runtime measurements. Using quantified-learning metrics—such as the Risk-of-Harm Index, tool complexity, and eco-impact—routers can dynamically select safe paths for a user's requests [64]. Critically, this runtime decision-making is constrained by the compile-time rules; a router can never execute a path that the CI/linting toolchain would have rejected. This creates a hierarchical integrity model that combines the certainty of static analysis with the flexibility of dynamic routing. To make these rights tangible, the framework maps them to domain-specific workflows within the Cybernetic Cookbook (`home.<em>`, `finance.</em>`, etc.), each governed by explicit neurorights predicates that forbid ideology enforcement and mandate retrieval-only access [64]. Specialized, highly restricted "pilot" workflows are defined for nanoswarm and neuroswarm research, ensuring that exploratory activities remain within safe, research-grade boundaries and never escalate to direct biological control .

Underpinning this entire structure is a governance layer built on provable identity and immutability. Every action is anchored to a user via a cryptographic authorship triple (`DID/ALN/Bostrom`), and all system configurations are hex-stamped for immutable auditing . This ensures accountability and allows for transparent verification of the system's operation. The entire system operates within a quantitative risk management framework, with the 0.3 risk-of-harm ceiling acting as a hard, non-negotiable limit on acceptable engagement [64]. This ceiling is calculated using a composite index likely incorporating neurophysiological data (from EEG and HRV) and other factors to provide a holistic measure of potential harm to the user. Ultimately, this framework successfully translates high-level ethical principles of neurorights—such as mental privacy, identity, and agency—into low-level, verifiable code and policy [33] [44]. It represents a paradigm shift towards a future where digital rights are not merely claimed but are engineered directly into the fabric of our technological environment, making them far more resilient to political, economic, or corporate pressures.

Reference

1. Proceedings of the 2025 Conference on Empirical Methods ... https://aclanthology.org/volumes/2025.emnlp-main/
2. Bounding Causal Effects and Counterfactuals https://arxiv.org/pdf/2508.13607

3. Improving economics and safety of water cooled reactors https://www-pub.iaea.org/MTCD/Publications/PDF/te_1290_prn.pdf
4. Numerical study of a convective cooling strategy for increasing ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10890868/
5. Human–Machine Interaction Using Probabilistic Neural ... https://www.mdpi.com/2079-9292/11/6/932
6. Enhancing the Security & Privacy of Wearable Brain- ... https://arxiv.org/pdf/2201.07711
7. Next Generation Risk Assessment approaches for ... https://www.sciencedirect.com/science/article/pii/S2452074824000338
8. User-Centered Redesign of Monitoring Alarms: A Pre–Post ... https://www.mdpi.com/2227-9032/13/23/3033
9. Validation of a Light EEG-Based Measure for Real-Time ... https://www.mdpi.com/2076-3425/12/3/304
10. Micro- and Nanoplastics Breach the Blood–Brain Barrier ... https://www.mdpi.com/2079-4991/13/8/1404
11. Proceedings of the ICR'22 International Conference on ... https://link.springer.com/content/pdf/10.1007/978-3-031-14054-9.pdf
12. Health Monitoring Systems-An Enabling Technology For ... https://www.scribd.com/document/683664059/Health-Monitoring-Systems-An-Enabling-Technology-for-Patient-Care-R-Gupta-and-D-Biswas-CRC-Press-2020
13. Zbirka-ITI-20231.pdf https://www.researchgate.net/profile/Grigorij_Gnatienko/publication/383500444_Zbirka_ITI_20231/links/66d073cf2390e50b2c1d8879/Zbirka-ITI-20231.pdf
14. 英汉电子和通信产业 https://www.scribd.com/document/669392670/20180611202740-61580
15. West African Journal of Industrial & Academic Research https://www.researchgate.net/profile/Comfort-Olebara/publication/358822378_Simulation_of_Microcontroller_Behavior_for_Hardware_Backdoor_Detection_pg_14-27/links/62a2255055273755ebe07a9c/Simulation-of-Microcontroller-Behavior-for-Hardware-Backdoor-Detection-pg-14-27.pdf
16. Electroacoustical simulation of listening room acoustics for ... https://core.ac.uk/download/13720847.pdf
17. 978-1-63828-239-6 (1) For Electronics and Communication https://www.scribd.com/document/969422608/978-1-63828-239-6-1-for-electronics-and-communication
18. A Pilot Study using Covert Visuospatial Attention as an ... https://dl.acm.org/doi/abs/10.1145/3460421.3480420

19. A BCI Based Alerting System for Attention Recovery of UAV ... https://www.mdpi.com/1424-8220/21/7/2447
20. ICCIS 3.0 Volume-1 | PDF | Key (Cryptography) https://www.scribd.com/document/959924792/ICCIS-3-0-Volume-1
21. Tool Learning with Foundation Models https://dl.acm.org/doi/10.1145/3704435
22. Tool Learning with Foundation Models https://dl.acm.org/doi/full/10.1145/3704435
23. Spam Message Detector https://www.kaggle.com/code/dev0914sharma/spam-message-detector
24. Lessons Learned So Far From Verifying the Rust Standard ... https://arxiv.org/html/2510.01072v2
25. Lessons Learned So Far From a Community Effort to Verify ... https://arxiv.org/pdf/2510.01072
26. A Hybrid Approach to Semi-automated Rust Verification (... https://arxiv.org/pdf/2403.15122
27. A hybrid approach to semi-automated Rust verification https://arxiv.org/html/2403.15122v1
28. 333333 23135851162 the 13151942776 of 12997637966 ftp://ftp.cs.princeton.edu/pub/cs226/autocomplete/words-333333.txt
29. How does Rust achieve compile-time-only pointer safety? https://stackoverflow.com/questions/29628650/how-does-rust-achieve-compile-time-only-pointer-safety
30. Research Roadmap of Service Ecosystems: A Crowd ... https://www.sciopen.com/article/10.26599/IJCS.2022.9100026
31. Artificial Intelligence Applied to Battery Research: Hype or ... https://pmc.ncbi.nlm.nih.gov/articles/PMC9227745/
32. A comparative review on neuroethical issues in neuroscientific ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10536163/
33. Four ethical priorities for neurotechnologies and AI https://www.nature.com/articles/551159a
34. The functional differentiation of brain–computer interfaces ... https://www.nature.com/articles/s41599-023-02419-x
35. (PDF) Addressing privacy risk in neuroscience data https://www.researchgate.net/publication/363415171_Addressing_privacy_risk_in_neuroscience_data_from_data_protection_to_harm_prevention
36. (PDF) Neurorights, Mental Privacy, and Mind Reading https://www.researchgate.net/publication/382079309_Neurorights_Mental_Privacy_and_Mind_Reading

37. Is the European Data Protection Regulation sufficient to deal ... https://academic.oup.com/jlb/article/7/1/lsaa051/5864051
38. (PDF) Neurorights in the Constitution https://www.researchgate.net/publication/385097579_Neurorights_in_the_Constitution_from_neurotechnology_to_ethics_and_politics
39. The new regulation of non-medical neurotechnologies in ... https://www.researchgate.net/publication/384334751_The_new_regulation_of_non-medical_neurotechnologies_in_the_European_Union_overview_and_reflection
40. Can Rust const generics use trait bounds with an inequality ... https://stackoverflow.com/questions/79591114/can-rust-const-generics-use-trait-bounds-with-an-inequality-e-g-n2-n1
41. Functional Design Principles, Patterns, and Practices ... https://www.scribd.com/document/710822784/Functional-Design-Principles-Patterns-And-Practices-Robert-C-Martin-Z-Library
42. glove.6B.100d.txt-vocab.txt https://worksheets.codalab.org/rest/bundles/0xadf98bb30a99476ab56ebff3e462d4fa/contents/blob/glove.6B.100d.txt-vocab.txt
43. Arxiv今日论文| 2026-01-19 http://lonepatient.top/2026/01/19/arxiv_papers_2026-01-19.html
44. Neuroethics and Neurorights - PMC - PubMed Central - NIH https://pmc.ncbi.nlm.nih.gov/articles/PMC12688770/
45. After the Digital Tornado https://resolve.cambridge.org/core/services/aop-cambridge-core/content/view/B746434A076A9EC7FD10AF12D69E6EA4/9781108426633AR.pdf/After_the_Digital_Tornado.pdf?event-type=FTLA
46. Inhibitory Control and Brain–Heart Interaction: An HRV-EEG ... https://pmc.ncbi.nlm.nih.gov/articles/PMC9221218/
47. Stress Analysis Based on Simultaneous Heart Rate ... https://pmc.ncbi.nlm.nih.gov/articles/PMC8407658/
48. An Overview of Heart Rate Variability Metrics and Norms https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2017.00258/full
49. Prototype of a Multimodal Platform Including EEG and HRV ... https://www.mdpi.com/2227-9717/13/4/1074
50. (PDF) Heart Rate Variability Assessment by the Entropy ... https://www.researchgate.net/publication/363694743_Heart_Rate_Variability_Assessment_by_the_Entropy_Parameters_during_Sleep
51. Cross-Modal Computational Model of Brain-Heart ... https://arxiv.org/html/2601.06792v1

52. Cross-correlation of EEG frequency bands and heart rate ... https://pubmed.ncbi.nlm.nih.gov/21046273/
53. Identifying HRV and EEG correlates of well-being using ... https://www.researchgate.net/publication/378575562_Identifying_HRV_and_EEG_correlates_of_well-being_using_ultra-short_portable_and_low-cost_measurements
54. Resting EEG Microstates and Autonomic Heart Rate ... https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2018.00460/full
55. Entropy in Heart Rate Dynamics Reflects How HRV- ... https://www.mdpi.com/1099-4300/22/3/317
56. Trends in Heart-Rate Variability Signal Analysis - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC8522021/
57. Cross-correlation of EEG frequency bands and heart rate ... https://www.researchgate.net/publication/47662151_Cross-correlation_of_EEG_frequency_bands_and_heart_rate_variability_for_sleep_apnoea_classification
58. Dynamic brain-heart interaction in sleep characterized by ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12357881/
59. Artificial Intelligence in Science and Society: the Vision of ... https://www.researchgate.net/publication/387984873_Artificial_Intelligence_in_Science_and_Society_the_Vision_of_USERN
60. The Need for Expanded Legal Protections of Brain Data https://www.researchgate.net/publication/380493553_Safeguarding_Neural_Privacy_The_Need_for_Expanded_Legal_Protections_of_Brain_Data
61. Building brain-inspired computing | Nature Communications https://www.nature.com/articles/s41467-019-12521-x
62. (PDF) Brain-MCP: A Fully Homomorphic Neuro-Symbolic ... https://www.researchgate.net/publication/393129669_Brain-MCP_A_Fully_Homomorphic_Neuro-Symbolic_Protocol_for_Governing_System_3_Cognition_and_Restoring_Semantic_Scarcity
63. Futuresphere Annual 2025: Trust, Technology and Tomorrow https://assets.kpmg.com/content/dam/kpmgsites/au/pdf/2025/futuresphere-annual-report-2025.pdf
64. Artificial Intelligence in Science and Society: The Vision of ... https://ieeexplore.ieee.org/iel8/6287639/10820123/10839366.pdf

65. Andreas K. Engel, Karl Friston, JA Scott Kelso, Peter König ... https://www.academia.edu/2836204/Andreas_K_Engel_Karl_Friston_JA_Scott_Kelso_Peter_K%C3%B6nig_Ilona_Kov%C3%A1cs_Angus_MacDonald_III_Earl_K_Miller_William_A_Phillips_Steven_M_Silverstein_Catherine_Tallon_Baudry_Jochen_Triesch_and_Peter_Uhlhaas
66. A/HRC/57/61 - General Assembly - the United Nations https://docs.un.org/en/A/HRC/57/61
67. Neurorights in the Constitution: from neurotechnology to ethics ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11491849/
68. The right to mental integrity in the age of neurotechnology https://academic.oup.com/jlb/article/12/1/lsaf010/8156051
69. Full article: Neurotechnologies and human rights https://www.tandfonline.com/doi/full/10.1080/13642987.2024.2310830
70. Neurotechnology https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/advisorycommittee/neurotechnology/03-ngos/ac-submission-cso-neurorightsfoundation.pdf
71. Preliminary draft report of the IBC on ethical issues ... https://unesdoc.unesco.org/ark:/48223/pf0000375237
72. asbestos---hazards-and-safe-practice-for-clear-up-after- ... https://www.who.int/docs/default-source/chemical-safety/asbestos/asbestos---hazards-and-safe-practice-for-clear-up-after-tsunami.pdf
73. Radiation: Electromagnetic fields https://www.who.int/news-room/questions-and-answers/item/radiation-electromagnetic-fields
74. Laboratory biosafety manual https://iris.who.int/bitstreams/9e97e6c8-0955-46a9-b638-b4d0c9acbcd7/download
75. PHENOL HEALTH AND SAFETY GUIDE - IRIS https://iris.who.int/bitstream/handle/10665/39958/9241510889eng.pdf?sequence=1
76. tuberculosis laboratory biosafety manual - IRIS https://iris.who.int/bitstreams/97019147-67d0-450b-9d1b-2e7f5fce7be9/download
77. Internet of Things Based Automated Ceiling Fan Cleaning ... https://ieeexplore.ieee.org/abstract/document/10912397/
78. Neural Network For Risk Assessment In Life Insurance ... https://ieeexplore.ieee.org/document/10005386/
79. Risk Management: Pro-active Principles for Project Success https://ewh.ieee.org/r1/boston/rl/files/boston_rs_meeting_mar10.pdf