A Neuro-Cyber Exploitation and Reconnaissance Taxonomy (NeuroCERT) for Human-Centric Cybersecurity

Cengiz Acarturk[1], Melike Caglayan[1], Ece Caglayan[2], Anna Maria Wilkosz[1]

[1]Centre for Cognitive Science, Jagiellonian University, Poland
[2]Informatics Institute, Middle East Technical University
{cengiz.acarturk, melike.caglayan}@uj.edu.pl, cece@metu.edu.tr,
anna.wilkosz@doctoral.uj.edu.pl

Abstract

Neuroscientists and cyber threat actors operate on a "black box" paradigm, relying on both the passive measurement of physical exhaust to infer hidden internal states, and the active injection of targeted stimuli to disrupt or manipulate those systems. This paper introduces the Neuro-Cyber Exploitation and Reconnaissance Taxonomy (NeuroCERT), a theoretical framework that maps cybersecurity side-channel attacks and active vectors to psychophysiological measurement and neurostimulation techniques. It proposes that AI can serve as a translational layer to parse noisy biological data into actionable metrics or automate closed-loop attacks, suggesting the potential of novel threat vectors in human-centric cybersecurity.

1 Introduction

Modern computer networks and the human nervous system share fundamental architectural characteristics: both are complex, fortified, and largely opaque to external observers. A neuroscientist aiming to infer or alter perceptual and cognitive processes is akin to a threat actor attempting to deduce cryptographic states through passive monitoring or manipulate system execution via active fault injection. In both cases, the core challenge remains similar: both the neuroscientist and the threat actor operate under a "black box" paradigm, either measuring the interception of physical leakages to deduce hidden states or injecting interference to disrupt and hijack normal operations.

In cognitive sciences, researchers employ measurable physical proxies—such as electrical signals and hemodynamic activity—for passive observation alongside neurostimulation techniques to actively modulate brain functions, both for research and clinical purposes over the past several decades. In parallel, cybersecurity has witnessed a proliferation of hardware-based side-channel attacks, interface interception techniques, and active fault-injection methodologies. These methods provide future misuse scenarios that bypass software defense mechanisms by either measuring the physical "exhaust" of computation or actively inducing localized hardware faults.

Recent literature has begun to recognize the parallels between these domains, demonstrating that biological interfaces, such as EEG, can be exploited as side-channels to infer identity-related information from brain activity. For instance, ML (Machine Learning) models have achieved high biometric identification accuracies across multiple EEG signal datasets (Chen et al., 2020; Maiorana, 2020) [1]. EEG-based systems can also be used for inferring personality traits with CNN-LSTM and ResNet-LSTM architectures achieving high predictive performance (Xu et al., 2022). Similarly, peripheral sensing modalities such as eye tracking have been shown to encode specific behavioral and cognitive information. For instance, demographic attributes, cognitive load, and personality traits can be inferred from gaze dynamics (González et al., 2025; Salima et al., 2023; Tsigeman et al., 2024). In immersive environments, eye-movement biometrics enable user identification with high accuracy (Lohr & Komogortsev, 2022; Liebers et al., 2021; Rack et al., 2023). These findings support

[1] We use the term Machine Learning (ML) models to refer to neural models in a broad sense, including traditional ML models, as well as deep learning models and more recent models relying on transformer architectures.

Proceedings of the Second International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security (NLPAICS'2026)

the emerging paradigm of side-channel sensing, in that medical diagnostics and cyber-physical attacks operate on similar fundamental pipelines of signal discovery, sensing, and extraction.

Nevertheless, analogies are often insufficient and similarities may be misleading. Deeper analyses and theoretical frameworks are needed to reveal the potential to fill in the gaps and thus to bridge these fields in a comprehensible way. Currently, the literature lacks a unified taxonomy that maps both the observational mechanics of psychophysiological tools and the manipulative mechanics of neurostimulation to their cybersecurity counterparts. To address this gap, we present a theoretical framework aiming to map physiological data acquisition and modulation modalities to specific cyber-physical threat vectors, exhibiting a cross-disciplinary approach to systems analysis. This framework draws parallels between how researchers observe and influence brain activity, and how threat actors reconnoiter and exploit computer system vulnerabilities. In this framework, psychophysiological tools (e.g., EEG, fNIRS) and neurostimulation devices (e.g., TMS) mirror the spectrum of passive reconnaissance and active exploitation techniques used by attackers against a "black box" system. In this study, we present these mappings from a cognitive science point of view. To this end, we developed the *Neuro-Cyber Exploitation and Reconnaissance Taxonomy* (*NeuroCERT*), focusing on measurement modalities of human psychophysiology.

The NeuroCERT mappings were developed through comparison of psychophysiological modalities and cyber-physical vectors across four operational dimensions: signal accessibility, passive versus active operation, target layer (central or peripheral processing), and information leakage or intervention capability. The framework does not assume biological and computational systems are structurally identical. Instead, the taxonomy focuses on similarities in observation, inference, and manipulation mechanisms. NeuroCERT should therefore be interpreted as a theoretical threat-modeling framework rather than an empirical attack demonstration.

The modalities included in NeuroCERT differ substantially in accessibility and deployment feasibility. Peripheral sensing methods such as eye tracking, ECG, wearable sensing, and EDA may plausibly appear in consumer or workplace environments, whereas modalities including MEG, PET, fMRI, TMS, and DBS require specialized clinical or laboratory infrastructure. Accordingly, the framework includes both current and speculative scenarios, and many cited findings originate from controlled experimental settings rather than real-world adversarial deployments.

Unlike prior work focused on isolated topics such as BCI security, biometric privacy, or physiological authentication, NeuroCERT organizes psychophysiological sensing and neurostimulation methods according to shared cyber-physical operational patterns.

Below, we present a set of analogical mappings that establish the background to build the NeuroCERT taxonomy between human-centric physiological tools and cyber-attack vectors. We assume an architectural locus in that we group the taxonomy into two parts: *Central Processing Interception* (*Core*) and *Peripheral Processing Interception* (*Edge*). Within each architectural locus, we categorize the vectors by their operational mode: *Passive Reconnaissance Vectors* and *Active Exploitation Vectors*.

2 Central Processing Interception (Core)

Passive Reconnaissance Vectors

2.1 Packet Sniffing, Network Traffic Analysis, and Electroencephalography

Packet sniffing employs an interface (a monitor or a network interface) to capture (mostly encrypted) data packets flowing back and forth. If network traffic is heavily encrypted, the attacker cannot read the deep payload. However, by analyzing packet size, transmission frequency, and traffic flow metadata, the attacker can infer the system's state or the state of the application running, in a similar way to how neuroscientists use different electroencephalography (EEG) bands to infer cognitive states.

EEG uses electrodes on the scalp to measure electrical voltage fluctuations resulting from ionic current within the neuron groups (action potentials) across the surface of the brain. As the skull diffuses electrical signals, EEG relies on analyzing the frequencies and amplitudes (rhythms) of aggregated surface activity. EEG has good temporal resolution accompanied by relatively poor spatial resolution. Consequently, neither EEG nor packet sniffing can identify which deep structures (brain structure or data payload) cause the measured signal. However, both passively capture the rhythms (power vs. traffic volume, frequency, connectivity vs. packet source and destination headers), interpreted as indicators of the black box system activity.

The current research on EEG has revealed numerous contexts for obtaining various aspects of human traits. One specific domain is EEG-based biometric systems, aiming to identify individuals with high accuracy using deep convolutional architectures, current models exceeding 99% detection accuracy under specific contexts (Akbarnia & Daliri, 2024). EEG signals also enable inference of latent psychological traits such as personality and emotional states and mental health conditions such as depression and schizophrenia with high accuracies (Shoeibi et al., 2021). These studies indicate that the utilization of EEG as a method for *sniffing* human brain's electrophysiological data, directly enabling to target person identification, personality traits and mental states and disorders has been gaining increasing research interest.

2.2 Power-Analysis Side-Channels, Functional Near-Infrared Spectroscopy and Functional Magnetic Resonance Imaging

Side-channel attacks aim to measure the physical byproducts of computing passively. For instance, if a processor is executing a complex cryptographic algorithm, it draws more electrical power and emits more heat. A power analysis is used for tracking the processor's computations. Similarly, functional near-infrared spectroscopy (fNIRS) and functional magnetic resonance imaging (fMRI) measure hemodynamic activity (blood flow) in the brain by utilizing the BOLD (Blood-Oxygen-Level-Dependent) contrast. They detect changes in oxygenated vs. deoxygenated blood near the cortex surface. A higher consumption of oxygen is interpreted as typically increased neural activity in the brain, within the framework of the information-processing framework to study brain activity.

By observing changes in oxygen consumption, fNIRS and fMRI provide indirect access to neural activity, comparable to how power-analysis side channels rely on variations in energy usage to infer internal processing. The studies have shown that these hemodynamic responses follow consistent patterns across tasks and individuals. For instance, fNIRS data has been used to classify gender based on differences in cerebral blood flow during cognitive tasks (Hiwa et al., 2016; Hiroyasu et al., 2014). The findings indicate that blood flow signals contain information beyond immediate task execution, including demographic attributes not explicitly provided by the user.

The analogy also applies to identity-related information. Functional connectivity patterns derived from these measures signals enable identification of individuals with high accuracy, ranging from about 75% to over 99% depending on the method (De Souza Rodrigues et al., 2019; Novi et al., 2023). ML models, including convolutional architectures and representation-learning approaches, further improve identification performance (Sincan et al., 2017; Cai et al., 2021; Lu et al., 2024). This is akin to how power traces in hardware systems can reveal device-specific behavior in addition to ongoing computations.

In addition to identity, fNIRS and fMRI signals can reflect cognitive load and task demands, and classification mental workload, stress, and user intent from hemodynamic responses (Liu et al., 2021). The studies comparing different approaches report that deep-learning methods often achieve higher accuracy and can operate with reduced preprocessing requirements (Eastmond et al., 2022). Combining fNIRS and fMRI with other modalities allows models to further capture both spatial and temporal aspects of brain activity, improving identification and classification performance (Chen et al., 2022; Wang et al., 2019; Bhattacharya et al., 2025). This is similar to combining multiple physical signals in traditional side-channel analysis to obtain more precise information about a system's internal processes.

2.3 Electromagnetic Emanation Attacks and Magnetoencephalography

Electromagnetic emanation attacks, specifically known as TEMPEST or Van Eck Phreaking, aim to capture the electromagnetic radiation emanated from hardware (a CPU, monitor, or keyboard) from a distance. Magnetoencephalography (MEG) measures minute magnetic fields produced by the brain's electrical activity. The magnetic fields pass through the skull, giving MEG superior spatial mapping. Both MEG and TEMPEST require highly sensitive sensors (SQUIDs in MEG and sensitive antennas in TEMPEST) to approximate the data being processed. Specifically, MEG is comparable to electromagnetic emanation attacks, where weak magnetic signals are used to infer activity. Recent studies show that MEG signals contain sufficient information to recover high-level representations of visual input. For example, ML models can retrieve semantic features of viewed stimuli and, in some cases, generate recognizable image reconstructions (Seeliger et al., 2018; Vidaurre et al., 2021; Van De Nieuwenhuijzen et al., 2013). This is akin to how electromagnetic side-channel attacks reconstruct screen content or keystrokes from emitted signals. The use of ML models has improved the quality of these reconstructions and enabled accurate decoding of perceptual content from MEG signals (Seeliger et al., 2018; Vidaurre et al., 2021). These methods capture temporal patterns in neural activity, allowing the identification of what is being perceived alongside how information evolves over time. This temporal aspect is comparable to monitoring signal changes in electromagnetic emissions to infer computing processes.

2.4 Passive Telemetry Tracing and Positron Emission Tomography

In cybersecurity, passive telemetry tracing or dynamic taint analysis, where an observer tracks how a specific, known data packet flows through complex internal application logic. These techniques involve "tagging" a specific piece of data at the system's edge (like an untrusted user input) and tracking how it flows through the application's deep internal logic. Dynamic taint analysis is also similar to a Supply Chain Attack in that, in the latter, an attacker injects a malicious payload upstream and monitors its propagation into the networks of the target systems. This is analogous to positron emission tomography (PET) scans, which require injecting a radioactive tracer (usually a glucose analog) into the bloodstream and passively measuring the brain activity. As the brain consumes the glucose for energy, the scanner tracks the radioactive decay, showing where the injected material ended up deep within the brain's metabolic pathways. While PET requires the introduction of a biological tracer (usually a glucose analog), the observational phase is passive. The scanner tracks where the tracer propagates deep within the brain's metabolic pathways.

PET provides a direct way to observe how externally introduced signals propagate through biological systems. Recent studies have shown that metabolic activity patterns can be used to distinguish between different neurological and clinical conditions (Ryoo et al., 2024; Perovnik et al., 2022; Zhang et al., 2026). These approaches rely on identifying how the injected tracer is distributed across brain regions, which reflects underlying functional and structural differences. This is consistent with the idea of tracing how a marked input moves through a system and produces measurable internal states. ML methods further improve the analysis of PET data by enabling more precise segmentation and detection of metabolic activity across brain regions (Li et al., 2025; Shan et al., 2023; Zhang et al., 2021). By capturing spatial patterns of tracer uptake, these models allow a detailed mapping of how energy consumption varies across the brain. This may be interpreted as analogous to telemetry tracing, where observation of the input provides indirect information about internal system behavior.

In addition, clustering and pattern analysis applied to PET data have been used to group individuals based on metabolic phenotypes linked to clinical and psychological characteristics (Zhang et al., 2026). Although these approaches are primarily used in clinical contexts, they show that PET signals can reflect structured variations across individuals. This suggests that similar methods could be adapted to study more abstract traits, such as personality, even though direct work on personality-trait prediction using PET remains limited (Nudin et al., 2024).

Active Exploitation Vectors

2.5 Fault Injection and Transcranial Magnetic Stimulation

Fault injection (glitching) in hardware systems target precisely timed voltage drops or electromagnetic pulses, which introduce transient faults in a processor, causing instruction skips, corrupted data paths, or altered control flow (Bozzato et al., 2019; Menu et al., 2020; Gaine et al., 2023). These disturbances can bypass security checks or disrupt cryptographic routines without damaging the underlying hardware. Current glitching techniques allow fine-grained control over timing and intensity, allowing repeatable and targeted faults at specific execution points.

This mechanism mirrors transcranial magnetic stimulation (TMS), which applies rapidly changing magnetic fields to induce electrical currents in cortical tissue. A single pulse can trigger brief activation followed by inhibition, temporarily disrupting local processing and acting as a virtual lesion, where task performance linked to the targeted region is selectively impaired (Siebner et al., 2009; Pascual-Leone et al., 2000; Weissman-Fogel & Granovsky, 2019; Silvanto & Muggleton, 2008). When applied in a time-locked manner, TMS can interfere with specific processing stages, altering signal strength or signal-to-noise ratios without causing permanent damage (Silvanto et al., 2007; Silvanto & Cattaneo, 2017).

In both cases, the attack targets processing at a precise moment rather than modifying system structure. TMS perturbs neural computation during critical time windows, while fault injection disrupts instruction execution at specific clock cycles. The result is a localized and temporary deviation from normal processing, sufficient to alter system behavior without persistent changes.

2.6 Direct Memory Access Override and Deep Brain Stimulation

In direct memory access (DMA) override attacks, an adversary bypasses standard I/O controls to directly read or modify protected memory regions. This mechanism exhibits similarities to deep brain stimulation (DBS), which introduces signals into core processing circuits, and modulates system state without relying on typical sensory input pathways. High-frequency stimulation may alter ongoing neural dynamics, analogous to modifying memory contents or control flow at a low level (McIntyre & Anderson, 2016; Lozano et al., 2019; Jakobs et al., 2019). Unlike non-invasive methods, DBS operates through direct access to deep neural structures, bypassing peripheral sensory pathways.

Recent developments in adaptive or closed-loop DBS strengthen this comparison. These systems monitor neural activity in real time and adjust stimulation, thus creating a feedback-driven intervention that depends on current system state (Krauss et al., 2021; Cagnan et al., 2019; Neumann et al., 2023). This resembles state-aware DMA behavior, where memory access or modification is triggered dynamically based on system conditions.

From a cybersecurity point of view, DBS devices also introduce a direct control interface that could be misused. The previous studies indicate that unauthorized access to implanted devices could alter stimulation patterns, potentially affecting motor function, emotional states, or behavior (Rathore et al., 2019). In both biological and computational systems, direct access to the core system state, bypassing standard safeguards, creates a point of control over system behavior.

3 Peripheral Processing Interception (Edge)

Passive Reconnaissance Vectors

3.1 Keylogging, Clickjacking, Screen Scraping, and Eye Tracking

Keyloggers, clickjackers and screen scrapers target the I/O (Input/Output) layer of a computer rather than its CPU or memory. They track what the user is clicking or typing. Eye tracking records eye movements, which allow extracting information about the location and duration of fixations and saccades, which indicate the interaction between a user and an interface. Both methods use the recorded information for interpreting user intention. Recent studies show that ML models can infer user intent, demographic attributes, and cognitive states from gaze patterns and fixation dynamics (González et al., 2025; Gao et al., 2023; Miles et al., 2024). Personality traits can also be predicted from eye movements achieving above-chance to high accuracy depending on the task (Salima et al., 2023; Tsigeman et al., 2024; Vargas et al., 2024). Moreover, eye-movement biometrics have emerged as a powerful identification modality. Deep-learning systems using gaze behavior achieve identification accuracies above 95%, particularly in VR/AR settings (Lohr & Komogortsev, 2022; Makowski et al., 2021; Rack et al., 2023). These findings demonstrate that eye movements act as a side-channel leaking both transient cognitive states and identity information.

3.2 Throughput Analysis and Pupillometry

When monitoring encrypted communication channels, an attacker may not access payload data but can observe traffic volume and timing patterns. Sudden increases in throughput often indicate high-load processing events or state changes within the system. Recent work shows that ML applied to encrypted traffic metadata can detect anomalies, identify system activity, and infer operational states without decrypting the data itself (Shen et al., 2023; Khraisat & Alazab, 2021).

A similar principle appears in the context of pupillometry. Human pupils dilate in response to cognitive load, with larger dilations reflecting increased processing demands. This effect has been reported across tasks such as memory, language comprehension, and decision-making, where higher task demands produce stronger pupil responses (Van Der Wel & Van Steenbergen, 2018; Eckstein et al., 2017). These findings indicate that pupil size is a peripheral indicator of global processing intensity rather than specific task content (Joshi & Gold, 2019; Ebitz et al., 2019; Viglione et al., 2023). They also position pupillometry as a biological throughput signal that reflects the intensity of processing, as traffic volume reflects load in a network. In both cases, the underlying content remains hidden, yet aggregate patterns provide indirect access to internal system states.

3.3 Timing Attacks and Electrocardiogram

A response from a computer system can be measured by cryptographic timing attacks, in which an attacker monitors the clock cycles a computer takes to execute specific algorithms. Consequently, the attacker aims to measure the variations in CPU execution time to identify the mathematical state of cryptographic keys. A similar response from human body is measured by electrocardiogram (ECG), which measures the rhythmic electrical pacing of the heart, providing a baseline clock rate for the entire biological system. Variations in this rhythm are called heart rate variability (HRV), which indicate how the system is responding to external demands.

Recent studies have shown that ECG signals encode stable and identifiable temporal patterns. ML models, including bidirectional LSTM and GRU architectures, achieve identification accuracies in the range of 98–100% across multiple datasets (Zehir et al., 2024). Other approaches, such as capsule networks with wavelet transforms and lightweight CNNs, report similarly high performance, often exceeding 99% under controlled conditions (Boujnouni et al., 2022; Al-Jibreen et al., 2024). Cross-session models maintain strong performance even under temporal variation, indicating that ECG signals contain persistent timing signatures (Chen et al., 2024). From a cybersecurity perspective, ECG can be viewed as a biological timing side-channel under constrained conditions. Just as execution-time variations may reveal internal states in cryptographic systems, dynamics may indirectly reflect identity-related and physiological response patterns. In both cases, the signal itself is not the protected data, but its timing structure provides indirect access to it.

3.4 API Hooking and Electromyography

In software exploitation, an API hooking or system call interception refers to an attacker “hooking” into API calls (e.g., writing to a disk, opening a camera) just before the operating system executes them. This is also similar to actuator monitoring attacks in industrial control systems, aiming to observe electrical signals sent to the system output layer, such as robotic arms or valves, i.e. system “muscles”. This is similar to EMG, which measures the electrical potential generated by skeletal muscle cells (the biological actuator as an output layer).

Recent studies provide supporting evidence for this analogy, showing that electromyography (EMG) signals contain structured information about fine-grained motor activity. For instance, ML methods can approximate handwriting and keystroke patterns from forearm EMG signals. Combining forearm and wrist EMG data enables handwriting recognition with high accuracies (Tigrini et al., 2023). These findings have been extended to relevant domains of identification, such as airwriting, where characters are written without physical contact and other gestures (Tripathi et al., 2023; Chihi et al., 2020).

From a cybersecurity point of view, EMG can be viewed as an output-side side-channel that leaks both discrete actions and continuous behavioral patterns. This mirrors API hooking, where intercepted system calls provide indirect information about user activity without accessing internal program logic. As EMG captures signals after internal processing has been resolved into motor commands, it aligns with observing finalized outputs rather than intermediate states.

This distinction separates EMG from modalities such as EEG or fNIRS, which target internal cognitive activity. Instead, EMG provides access to executed actions, enabling reconstruction of user behavior even when higher-level signals are unavailable. Accordingly, EMG may provide a form of action-level leakage rather than direct access to internal cognitive states.

3.5 Passive Load Monitoring and Electrodermal Activity

In passive load monitoring, an observer tracks a system’s thermal output or fan speeds to deduce when the system is operating under high stress or approaching threshold limits. This is analogous to electrodermal activity (EDA) or galvanic skin response (GSR), which measures changes in the skin's electrical conductance. This information may be interpreted as the presence or absence of high arousal or stress, depending on the context.

The studies that employ ML methods have shown that EDA signals can be used to classify emotional arousal and stress states, including acute and chronic stress conditions with high accuracy, often ranging between 83% and 97% depending on the dataset and model (Raju et al., 2023; Li & Liu, 2020; Subathra et al., 2025; Kim et al., 2024).

These results indicate that EDA signals can act as indicators of internal state intensity, in a way that is comparable to monitoring system load through indirect physical measurements. EDA has also been explored in relation to personality and behavioral traits, although results are less consistent. Some studies show that combining galvanic skin response with other physiological signals, such as heart rate variability, can support prediction of personality traits like extraversion and conscientiousness (Tseng et al., 2023). In addition, EDA is widely used in wearable systems for continuous monitoring. Integrated GSR sensors can track stress and emotional states in real time, often combining EDA with other physiological signals to improve reliability (Golgouneh & Tarvirdizadeh, 2020; Majid et al., 2026; Kim et al., 2024). These multimodal approaches achieve higher accuracy, similar to combining multiple indicators in system monitoring to better estimate overall load.

Active Exploitation Vectors

3.6 Sensor Spoofing and Galvanic Vestibular Stimulation

Autonomous cyber-physical systems rely on sensors such as global positioning system (GPS), inertial measurement units (IMUs), and cameras to estimate position and motion. In sensor spoofing attacks, an adversary injects false but internally consistent signals into these sensors, causing the system to misinterpret its environment. For example, GPS spoofing can redirect drones or introduce gradual trajectory deviations without triggering immediate detection (Khan et al., 2021; Dasgupta et al., 2024).

Mode	Modality	Analogue	Context
C&P	EEG	Packet Sniffing	Consumer / Research
	fNIRS, fMRI	Power-Analysis Side-Channels	Research / Clinical
	MEG	Electromagnetic Emanation Attacks	Laboratory
	PET	Telemetry Tracing Analogy	Clinical
C&A	TMS	Fault Injection	Laboratory / Clinical
	DBS	DMA Override Analogy	Clinical implantation
E&P	Eye Tracking	Keylogging, Clickjacking, Screen Scraping	Consumer / VR
	Pupillometry	Throughput Analysis	Consumer / Research / VR
	ECG	Timing-Based Leakage	Wearables / Medical
	EMG	API-Hooking Analogy	Wearables / Research
	EDA	Passive Load Monitoring	Wearables
E&A	GVS	Sensor Spoofing	Laboratory / VR

Table 1: Neuro-Cyber Exploitation and Reconnaissance Taxonomy (NeuroCERT). C: Core, P: Passive

This mechanism parallels galvanic vestibular stimulation (GVS), which involves applying electrical current to the vestibular nerve to actively distort the subject's sense of balance and spatial orientation. The vestibular system provides internal motion cues that support navigation and spatial awareness; disrupting this input leads to misperceptions of movement, postural instability, and navigation errors (Zwergal et al., 2024; Allred et al., 2024). Controlled GVS can induce virtual sensations of rotation and tilt without physical motion, effectively creating artificial self-motion signals (Gallagher et al., 2023; Pradhan et al., 2022).

In both cases, the attack targets the sensing layer rather than internal control logic. GVS introduces artificial vestibular input that the brain treats as real motion, while sensor spoofing feeds manipulated telemetry into navigation systems. The result is a distorted estimate of position and orientation, leading to disorientation or misnavigation even though the processing operates as expected.

Building upon the analogical mappings established in this section, the next section presents a taxonomy of mapping between psychophysiological measurement tools and cyber-attack vectors.

4 Neuro-Cyber Exploitation and Reconnaissance Taxonomy (NeuroCERT)

The NeuroCERT framework categorizes these methodologies across three primary axes: the Target Layer (Central Processing vs. Peripheral Processing), the Mode of Operation (Passive Reconnaissance vs. Active Exploitation), and the Vector/Analogue Pairing. While passive reconnaissance relies on measuring physical "exhaust" to deduce hidden states without alerting the system, active exploitation involves the targeted injection of electrical energy or stimuli to disrupt, alter, or hijack those internal states.

By aligning neuroscientific and other biological data acquisition techniques and neurostimulation with cyber-physical threat vectors, we aim to isolate the specific mechanisms of vulnerability within human-centric systems. The NeuroCERT taxonomy is presented in Table 1.

5 Discussion

Establishing the bridge between cognitive neuroscience and cybersecurity necessitates a unified approach to threat modeling. The NeuroCERT framework demonstrates that the human nervous system and computing networks may share fundamental architectural vulnerabilities. By mapping both passive reconnaissance and active manipulation vectors, this taxonomy provides a framework to anticipate and defend against the next generation of human-centric cyber-physical threats.

AI serves as the translational layer by providing ML-based analysis tools, bridging the gap between psychophysiological data and actionable metrics. AI/ML methods may support the interpretation of physiological and behavioral signals under controlled conditions. Within human-centric cybersecurity, multimodal systems combining physiological, behavioral, and linguistic information may support user-state inference, adaptive authentication, or behavioral profiling. These models have been increasingly utilized to map surface-level physiological telemetry back to specific cognitive states. Contemporary models have been demonstrating significant efficacy in predicting and interpreting brain responses (e.g., Wang et al., 2019; Tang et al., 2023). As analytical methods converge across these domains, AI-based noise-reduction techniques will refine the extraction of actionable signals.

Some future misuse scenarios may involve physiological systems integrated into wearable, VR/AR, or neuroadaptive technologies. Despite advances in physiological signal analysis, modality-specific limitations remain. MEG decoding is constrained by limited spatial resolution, dependence on pretrained models, and substantial inter-subject variability, with many studies relying on controlled experimental settings (Cicmil et al., 2014) and subject cooperation (Tang et al., 2023). Recent multimodal and AI-assisted approaches combining MEG with external representations or additional sensing modalities have improved decoding robustness and performance (Li et al., 2024; Maleki & Karimi-Rouzbahani, 2025). Nevertheless, many MEG-based inference scenarios remain experimental rather than operational.

Finally, while these analogies provide a powerful heuristic framework, they also present limitations and can sometimes be misleading. Despite the current success of ML algorithms in imitating human behavior, human neural architectures and neural ML models fundamentally share minimal similarities. These intersections are strictly limited to the behavioral level. The adoption of terminology such as "attention mechanisms" or "long short-term memory" in AI often reflects misnomers inherited from the von Neumann architecture. This shared terminology risks misleading researchers into overinterpreting behavioral successes as evidence of architectural isomorphism between natural and artificial cognitive systems. Therefore, establishing a bridge between natural and artificial cognitive systems is better achieved by utilizing ML models as a tool for a "systems" approach, rather than seeking direct similarities between their architectures. Ultimately, this study exemplifies such a systems approach, aiming to properly contextualize the convergence of cognitive neuroscience and cybersecurity.

References

Aaron R. Allred, Caroline R. Austin, Lanna Klausing, Nicholas Boggess, and Torin K. Clark. 2024. Human perception of self-motion and orientation during galvanic vestibular stimulation and physical motion. *PLOS Computational Biology*, 20(11):e1012601.

Afshin Shoeibi, Delaram Sadeghi, Parisa Moridian, Navid Ghassemi, Jónathan Heras, Roohallah Alizadehsani, Ali Khadem, Yinan Kong, Saeid Nahavandi, Yu-Dong Zhang, and Juan Manuel Gorriz. 2021. Automatic Diagnosis of Schizophrenia in EEG Signals Using CNN-LSTM Models. *Frontiers in Neuroinformatics*, 15:777977.

Alexandre Menu, Jean-Max Dutertre, Olivier Potin, Jean-Baptiste Rigaud, and Jean-Luc Danger. 2020. Experimental Analysis of the Electromagnetic Instruction Skip Fault Model. In *2020 15th Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, pages 1–7. IEEE.

Alireza Golgouneh and Bahram Tarvirdizadeh. 2020. Fabrication of a portable device for stress monitoring using wearable sensors and soft computing algorithms. *Neural Computing and Applications*, 32(11):7515–7537.

Alvaro Pascual-Leone, Vincent Walsh, and John Rothwell. 2000. Transcranial magnetic stimulation in cognitive neuroscience – virtual lesion, chronometry, and functional connectivity. *Current Opinion in Neurobiology*, 10(2):232–237.

Andrea Tigrini, Federica Verdini, Mara Scattolini, Federico Barbarossa, Laura Burattini, Micaela Morettini, Sandro Fioretti, and Alessandro Mengarelli. 2023. Handwritten Digits Recognition From sEMG: Electrodes Location and Feature Selection. *IEEE Access*, 11:58006–58015.

Andreas Zwergal, Denis Grabova, and Florian Schöberl. 2024. Vestibular contribution to spatial orientation and navigation. *Current Opinion in Neurology*, 37(1):52–58.

Andres M. Lozano, Nir Lipsman, Hagai Bergman, Peter Brown, Stephan Chabardes, Jin Woo Chang, Keith Matthews, Cameron C. McIntyre, Thomas E. Schlaepfer, Michael Schulder, Yasin Temel, Jens Volkmann, and Joachim K. Krauss. 2019. Deep brain stimulation: current challenges and future directions. *Nature Reviews Neurology*, 15(3):148–160.

Ansam Khraisat and Ammar Alazab. 2021. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4(1):18.

Aurelia Viglione, Raffaele Mazziotti, and Tommaso Pizzorusso. 2023. From pupil to the brain: New insights for studying cortical plasticity through pupillometry. *Frontiers in Neural Circuits*, 17.

Ayalapogu Ratna Raju, R. Ramadevi, Padamata Ramesh Babu, and Vetriselvi D. 2023. Galvanic Skin Response based Stress Detection System using Machine Learning and IoT. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pages 709–714. IEEE.

Awabed Al-Jibreen, Saad Al-Ahmadi, Saiful Islam & Abdel Momin Artoli. 2024. Person identification with arrhythmic ECG signals using deep convolution neural network. *Scientific Reports*, 14.

Ayush Tripathi, A. P. Prathosh, Suriya Prakash Muthukrishnan, and Lalan Kumar. 2023. SurfMyoAiR: A Surface Electromyography-Based Framework for Airwriting Recognition. *IEEE Transactions on Instrumentation and Measurement*, 72:1–12.

Becket R. Ebitz and Tirin Moore. 2019. Both a Gauge and a Filter: Cognitive Modulations of Pupil Size. *Frontiers in Neurology*, 9.

Biao Cai, Gemeng Zhang, Aiying Zhang, Li Xiao, Wenxing Hu, Julia M. Stephen, Tony W. Wilson, Vince D. Calhoun, and Yu-Ping Wang. 2021. Functional connectome fingerprinting: Identifying individuals and predicting cognitive functions via autoencoder. *Human Brain Mapping*, 42(9):2691–2705.

Cameron C. McIntyre and Ross W. Anderson. 2016. Deep brain stimulation mechanisms: the control of network activity via neurochemistry modulation. *Journal of Neurochemistry*, 139(S1):338–345.

Christian Rack, Tamara Fernando, Murat Yalcin, Andreas Hotho, and Marc Erich Latoschik. 2023. Who is Alyx? A new behavioral biometric dataset for user identification in XR. *Frontiers in Virtual Reality*, 4.

Chun-Hsiung Tseng, Hao-Chiang Koong Lin, Andrew Chih-Wei Huang, and Jia-Rou Lin. 2023. Personalized programming education: Using machine learning to boost learning performance based on students' personality traits. *Cogent Education*, 10(2).

Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini. 2019. Shaping the Glitch: Optimizing Voltage Fault Injection Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(2):199–224.

Clément Gaine, Pierre-Alain Moellic, Olivier Potin, and Jean-Max Dutertre. 2023. Fault Injection on Embedded Neural Networks: Impact of a Single

Instruction Skip. In *2023 26th Euromicro Conference on Digital System Design (DSD)*, pages 317–324. IEEE.

Condell Eastmond, Aseem Subedi, Suvranu De, and Xavier Intes. 2022. Deep learning in fNIRS: a review. *Neurophotonics*, 9(04):41411.

Diego Vidaurre, Radoslaw M Cichy, and Mark W Woolrich. 2021. Dissociable Components of Information Encoding in Human Perception. *Cerebral Cortex*, 31(12):5664–5675.

Dillon Lohr and Oleg V. Komogortsev. 2022. Eye Know You Too: Toward Viable End-to-End Eye Movement Biometrics for User Authentication. *IEEE Transactions on Information Forensics and Security*, 17:3151–3164.

Dongyang Li, Shiying Li, Quanying Liu, Chen Wei, and Jiachen Zou. 2024. Visual Decoding and Reconstruction via EEG Embeddings with Guided Diffusion. In *Advances in Neural Information Processing Systems 37*, pages 102822–102864, San Diego, California, USA. Neural Information Processing Systems Foundation, Inc. (NeurIPS).

Elena Parra Vargas, Lucia Amalia Carrasco-Ribelles, Javier Marin-Morales, Carla Ayuso Molina, and Mariano Alcañiz Raya. 2024. Feasibility of virtual reality and machine learning to assess personality traits in an organizational environment. *Frontiers in Psychology*, 15.

Elina Tsigeman, Viktoria Zemliak, Maxim Likhanov, Kostas A. Papageorgiou, and Yulia Kovas. 2024. AI can see you: Machiavellianism and extraversion are reflected in eye-movements. *PLOS ONE*, 19(8):e0308631.

Emanuele Maiorana. 2020. Deep learning for EEG-based biometric recognition. *Neurocomputing*, 410:374–386.

Gabriella Miles, Melvyn Smith, Nancy Zook, and Wenhao Zhang. 2024. EM-COGLOAD: An investigation into age and cognitive load detection using eye tracking and deep learning. *Computational and Structural Biotechnology Journal*, 24:264–280.

Gaurav N. Pradhan, Raquel Galvan-Garza, Alison M. Perez, Jamie Bogle, and Michael J. Cevette. 2022. Generating Flight Illusions Using Galvanic Vestibular Stimulation in Virtual Reality Flight Simulations. *Frontiers in Neuroergonomics*, 3.

Hartwig R. Siebner, Gesa Hartwigsen, Tanja Kassuba, and John C. Rothwell. 2009. How does transcranial magnetic stimulation modify neuronal activity in the brain? Implications for studies of cognition. *Cortex*, 45(9):1035–1042.

Hatem Zehir, Toufik Hafs, and Sara Daas. 2024. Empirical mode decomposition-based biometric identification using GRU and LSTM deep neural networks on ECG signals. *Evolving Systems*, 15(6):2193–2209.

Hayriye Cagnan, Timothy Denison, Cameron McIntyre, and Peter Brown. 2019. Emerging technologies for improved deep brain stimulation. *Nature Biotechnology*, 37(9):1024–1033.

Heena Rathore, Abdulla Khalid Al-Ali, Amr Mohamed, Xiaojiang Du, and Mohsen Guizani. 2019. A Novel Deep Learning Strategy for Classifying Different Attack Patterns for Deep Brain Implants. *IEEE Access*, 7:24154–24164.

Hong Gao, Lisa Hasenbein, Efe Bozkir, Richard Göllner, and Enkelejda Kasneci. 2023. Exploring Gender Differences in Computational Thinking Learning in a VR Classroom: Developing Machine Learning Models Using Eye-Tracking Data and Explaining the Models. *International Journal of Artificial Intelligence in Education*, 33(4):929–954.

Hun-gyeom Kim, Solwoong Song, Baek Hwan Cho, and Dong Pyo Jang. 2024. Deep learning-based stress detection for daily life use using single-channel EEG and GSR in a virtual reality interview paradigm. *PLOS ONE*, 19(7):e0305864.

Hyun Gee Ryoo, Hongyoon Choi, Kuangyu Shi, Axel Rominger, Dong Young Lee, and Dong Soo Lee. 2024. Distinct subtypes of spatial brain metabolism patterns in Alzheimer's disease identified by deep learning-based FDG PET clusters. *European Journal of Nuclear Medicine and Molecular Imaging*, 51(2):443–454.

Imane El Boujnouni, Hassan Zili, Abdelhak Tali, Tarik Tali, and Yassin Laaziz. 2022. A wavelet-based capsule neural network for ECG biometric identification. *Biomedical Signal Processing and Control*, 76:103692.

Ines Chihi, Ernest N. Kamavuako, and Mohamed Benrejeb. 2020. Modeling simple and complex handwriting based on EMG signals. In *Control Theory in Biomedical Engineering*, pages 129–149. Elsevier.

Irit Weissman-Fogel and Yelena Granovsky. 2019. The "virtual lesion" approach to transcranial magnetic stimulation: studying the brain–behavioral relationships in experimental pain. *PAIN Reports*, 4(4):e760.

J. X. Chen, Z. J. Mao, W. X. Yao, and Y. F. Huang. 2020. EEG-based biometric identification with convolutional neural network. *Multimedia Tools and Applications*, 79(15–16):10655–10675.

Jerry Tang, Amanda LeBel, Shailee Jain, and Alexander G. Huth. 2023. Semantic reconstruction of continuous language from non-invasive brain recordings. *Nature Neuroscience*, 26: 858–866.

Jiayu Lu, Tianyi Yan, Lan Yang, Xi Zhang, Jiaxin Li, Dandan Li, Jie Xiang, and Bin Wang. 2024. Brain fingerprinting and cognitive behavior predicting using functional connectome of high inter-subject variability. *NeuroImage*, 295:120651.

Jinfan Zhang, Fuchang Han, Xueying Wang, Feifei Wu, Xinyu Song, Qing Liu, Junling Wang, Alessandro Grecucci, Yuanchao Zhang, Xiaoping Yi, and Bihong T. Chen. 2026. Brain metabolic imaging with 18 F-PET-CT and machine-learning clustering analysis reveal divergent metabolic phenotypes in patients with amyotrophic lateral sclerosis. *European Journal of Nuclear Medicine and Molecular Imaging*, 53(3):2018–2033.

Joachim K. Krauss, Nir Lipsman, Tipu Aziz, Alexandre Boutet, Peter Brown, Jin Woo Chang, Benjamin Davidson, Warren M. Grill, Marwan I. Hariz, Andreas Horn, Michael Schulder, Antonios Mammis, Peter A. Tass, Jens Volkmann, and Andres M. Lozano. 2021. Technology of deep brain stimulation: current status and future directions. *Nature Reviews Neurology*, 17(2):75–87.

Jonathan Liebers, Patrick Horn, Christian Burschik, Uwe Gruenefeld, and Stefan Schneegass. 2021. Using Gaze Behavior and Head Orientation for Implicit Identification in Virtual Reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology*, pages 1–9, New York, NY, USA. ACM.

Juha Silvanto and Neil G. Muggleton. 2008. New light through old windows: Moving beyond the “virtual lesion” approach to transcranial magnetic stimulation. *NeuroImage*, 39(2):549–552.

Juha Silvanto and Zaira Cattaneo. 2017. Common framework for “virtual lesion” and state-dependent TMS: The facilitatory/suppressive range model of online TMS effects on behavior. *Brain and Cognition*, 119:32–38.

Juha Silvanto, Neil G. Muggleton, Alan Cowey, and Vincent Walsh. 2007. Neural adaptation reveals state-dependent effects of transcranial magnetic stimulation. *European Journal of Neuroscience*, 25(6):1874–1881.

Júlia de Souza Rodrigues, Fernanda Lenita Ribeiro, João Ricardo Sato, Rickson Coelho Mesquita, and Claudinei Eduardo Biazoli Júnior. 2019. Identifying individuals using fNIRS-based cortical connectomes. *Biomedical Optics Express*, 10(6):2889.

Junda Xu, Chi Zhou, and Qi Shao. 2022. ResNet-LSTM Model Based Big Five Personality Prediction System. In *Proceedings of the 4th International Conference on Intelligent Science and Technology*, pages 25–33, New York, NY, USA. ACM.

Katja Seeliger, Matthias Fritsche, Umut Güçlü, Sanne Schoenmakers, J-M. Schoffelen, Sander E. Bosch, and M. A. J. Van Gerven. 2018. Convolutional neural network-based encoding and decoding of visual object recognition in space and time. *NeuroImage*, 180:253–266.

Lebo Wang, Kaiming Li, Xu Chen, and Xiaoping P. Hu. 2019. Application of Convolutional Recurrent Neural Network for Individual Recognition Based on Resting State fMRI Data. *Frontiers in Neuroscience*, 13.

M. Gallagher, F. Romano, C.J. Bockisch, E.R. Ferrè, and G. Bertolini. 2023. Quantifying virtual self-motion sensations induced by galvanic vestibular stimulation. *Journal of Vestibular Research*, 33(1):21–30.

Maria K. Eckstein, Belén Guerra-Carrillo, Alison T. Miller Singley, and Silvia A. Bunge. 2017. Beyond eye gaze: What else can eyetracking reveal about cognition and cognitive development? *Developmental Cognitive Neuroscience*, 25:69–91.

Marieke E. van de Nieuwenhuijzen, A. R. Backus, Ali Bahramisharif, Christian F. Doeller, Ole Jensen, and Marcel AJ van Gerven.2013. MEG-based decoding of the spatiotemporal dynamics of visual category perception. *NeuroImage*, 83:1063–1073.

Martin Jakobs, Anton Fomenko, Andres M Lozano, and Karl L Kiening. 2019. Cellular, molecular, and clinical mechanisms of action of deep brain stimulation—a systematic review on established indications and outlook on future developments. *EMBO Molecular Medicine*, 11(4).

Matej Perovnik, An Vo, Nha Nguyen, Jan Jamšek, Tomaž Rus, Chris C. Tang, Maja Trošt, and David Eidelberg. 2022. Automated differential diagnosis of dementia syndromes using FDG PET and machine learning. *Frontiers in Aging Neuroscience*, 14.

Meftah Salima, Sahnoun M’hammed, Mourad Messaadia, and Sidi Mohamed Benslimane. 2023. Machine Learning for Predicting Personality Traits from Eye Tracking. In *2023 International Conference on Decision Aid Sciences and Applications (DASA)*, pages 126–130. IEEE.

Meng Shen, Ke Ye, Xingtong Liu, Liehuang Zhu, Jiawen Kang, Shui Yu, Qi Li, and Ke Xu. 2023. Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 25(1):791–824.

Muhammad Majid, Aamir Arsalan, Jaroslav Frnda, and Syed Muhammad Anwar. 2026. A Multimodal Perceived Stress Classification Framework Using Wearable Physiological Sensors. *IEEE Open Journal of the Computer Society*, 7:202–213.

Nela Cicmil, Holly Bridge, Andrew J. Parker, Mark W. Woolrich, and Kristine Krug. 2014. Localization of MEG human brain responses to retinotopic visual stimuli with contrasting source reconstruction approaches. *Frontiers in Neuroscience*, 8.

Nima Maleki and Hamid Karimi-Rouzbahani. 2025. Identifying Explainable and Generalizable Features for MEG Decoding. *bioRxiv*, 2025-04**.**

Ozge Mercanoglu Sincan, Hacer Yalım Keles, Yagmur Kır, Adnan Kusman, and Bora Baskak. 2017. Person identification using functional near-infrared spectroscopy signals using a fully connected deep neural network. *Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering*, *59*(2):55-68.

P. Subathra, S. Malarvizhi, K. Ferents Koni Jiavana, and Shantanu Patil. 2025. A Wearable Electronic Band for Stress Understanding Using Machine Learning. *IEEE Sensors Journal*, 25(20):38639–38648.

Pablo Villanueva González, Cristobal Subiabre Cuevas, Lino Jeldez, Benjamin Torrealba Troncoso, María Flavia Guiñazú, and Juan D. Velásquez. 2025. A gender-aware saliency prediction system for web interfaces using deep learning and eye-tracking data. *Brain Informatics*, 12(1):25.

Pauline van der Wel and Henk van Steenbergen. 2018. Pupil dilation as an index of effort in cognitive control tasks: A review. *Psychonomic Bulletin & Review*, 25(6):2005–2015.

Qinming Zhang, Yi Liao, Xiawan Wang, Teng Zhang, Jianhua Feng, Jianing Deng, Kexin Shi, Lin Chen, Liu Feng, Mindi Ma, Le Xue, Haifeng Hou, Xiaofeng Dou, Congcong Yu, Lei Ren, Yao Ding, Yufei Chen, Shuang Wu, Zexin Chen, et al. 2021. A deep learning framework for 18F-FDG PET imaging diagnosis inpediatric patients with temporal lobe epilepsy. *European Journal of Nuclear Medicine and Molecular Imaging*, 48(8):2476–2485.

Russell Li and Zhandong Liu. 2020. Stress detection using deep neural networks. *BMC Medical Informatics and Decision Making*, 20(S11):285.

Sagar Dasgupta, Abdullah Ahmed, Mizanur Rahman, and Thejesh N. Bandi. 2024. Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience. *arXiv preprint arXiv:2401.01394*.

Salamun Rohman Nudin, Rahmat Gernowo, Maman Somantri, and Adi Wibowo. 2024. Multi Task Classification Using Deep Learning Approaches for Big Five Personality Traits Prediction: A Review. In *2024 11th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, pages 37–42. IEEE.

Satoru Hiwa, Kenya Hanawa, Ryota Tamura, Keisuke Hachisuka, and Tomoyuki Hiroyasu. 2016. Analyzing Brain Functions by Subject Classification of Functional Near-Infrared Spectroscopy Data Using Convolutional Neural Networks Analysis. *Computational Intelligence and Neuroscience*, 2016:1–9.

Saurabh Bhattacharya, Sashikanta Prusty, Sanjay P. Pande, Monali Gulhane, Santosh H. Lavate, Nitin Rakesh, and Saravanan Veerasamy. 2025. Integration of multimodal imaging data with machine learning for improved diagnosis and prognosis in neuroimaging. *Frontiers in Human Neuroscience*, 19.

Sergio Luiz Novi Junior, Alex De Castro Carvalho, Rodrigo M. Menezes Forti, Fernado Cendes, Clarissa L. Yasuda, and Rickson C. Mesquita. 2023. Revealing the spatiotemporal requirements for accurate subject identification with resting-state functional connectivity: a simultaneous fNIRS-fMRI study. *Neurophotonics*, 10(01).

Shah Zahid Khan, Mujahid Mohsin, and Waseem Iqbal. 2021. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science*, 7:e507.

Siddhartha Joshi and Joshua I Gold. 2019. Pupil size as a window on neural substrates of cognition. *Trends in cognitive sciences,* 24.6: 466-480.

Silvia Makowski, Paul Prasse, David R. Reich, Daniel Krakowczyk, Lena A. Jager, and Tobias Scheffer. 2021. DeepEyedentificationLive: Oculomotoric Biometric Identification and Presentation-AttackDetection Using Deep Neural Networks. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(4):506–518.

Tomoyuki Hiroyasu, Kenya Hanawa, and Utako Yamamoto. 2014. Gender classification of subjects from cerebral blood flow changes using Deep Learning. In *2014 IEEE Symposium on Computational Intelligence and Data Mining (CIDM)*, pages 229–233. IEEE.

Wenbo Li, Zhenxing Huang, Hongyan Tang, Yaping Wu, Yunlong Gao, Jing Qin, Jianmin Yuan, Yang Yang, Yan Zhang, Na Zhang, Hairong Zheng, Dong Liang, Meiyun Wang, and Zhanli Hu. 2025. A generative whole-brain segmentation model for positron emission tomography images. *EJNMMI Physics*, 12(1):15.

Wolf-Julian Neumann, Andreas Horn, and Andrea A. Kühn. 2023. Insights and opportunities for deep brain stimulation as a brain circuit intervention. *Trends in Neurosciences*, 46(6):472–487.

Xin-Hua Chen, Yih-Liang Shen, and Tai-Shih Chi. 2024. Single-Lead ECG Cross-Session Identification Based on Conditional Domain Adversarial Network. *IEEE Sensors Journal*, 24(11):17865–17875.

Yasaman Akbarnia and Mohammad Reza Daliri. 2024. EEG-based identification system using deep neural networks with frequency features. *Heliyon*, 10(4):e25999.

Yi Shan, Shao-zhen Yan, Zhe Wang, Bi-xiao Cui, Hong-wei Yang, Jian-min Yuan, Ya-yan Yin, Feng Shi, and Jie Lu. 2023. Impact of brain segmentation methods on regional metabolism quantification in 18F-FDG PET/MR analysis. *EJNMMI Research*, 13(1):79.

Yuhao Chen, Jiajun Liu, Yaxi Peng, Ziyi Liu, and Zhipeng Yang. 2022. Multilayer Functional Connectome Fingerprints: Individual Identification via Multimodal Convolutional Neural Network. *Intelligent Automation & Soft Computing*, 33(3):1501–1516.

Ziming Liu, Jeremy Shore, Miao Wang, Fengpei Yuan, Aaron Buss, and Xiaopeng Zhao. 2021. A systematic review on hybrid EEG/fNIRS in brain-computer interface. *Biomedical Signal Processing and Control*, 68:102595.