Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges

SERGIO LÓPEZ BERNAL, University of Murcia, Departamento de Ingeniería de la Información y las Comunicaciones
ALBERTO HUERTAS CELDRÁN, Waterford Institute of Technology, Telecommunication Software and Systems Group and Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH
GREGORIO MARTÍNEZ PÉREZ, University of Murcia, Departamento de Ingeniería de la Información y las Comunicaciones
MICHAEL TAYNNAN BARROS, University of Essex, School of Computer Science and Electronic Engineering and Tampere University, CBIG/BioMediTech in the Faculty of Medicine and Health Technology
SASITHARAN BALASUBRAMANIAM, Waterford Institute of Technology, Telecommunication Software and Systems Group and RCSI University of Medicine and Health Sciences, FutureNeuro, SFI Research Centre for Chronic and Rare Neurological Diseases

Brain-Computer Interfaces (BCIs) have significantly improved the patients' quality of life by restoring damaged hearing, sight, and movement capabilities. After evolving their application scenarios, the current trend of BCI is to enable new innovative brain-to-brain and brain-to-the-Internet communication paradigms. This technological advancement generates opportunities for attackers, since users' personal information and physical integrity could be under tremendous risk. This work presents the existing versions of the BCI life-cycle and homogenizes them in a new approach that overcomes current limitations. After that, we offer a qualitative characterization of the security attacks affecting each phase of the BCI cycle to analyze their impacts and countermeasures documented in the literature. Finally, we reflect on lessons learned, highlighting research trends and future challenges concerning security on BCIs.

This work has been supported by the Irish Research Council under the government of Ireland post-doc fellowship (Grant No. GOIPD/2018/466), by the Science Foundation Ireland (SFI) under Grant No. 16/RC/3948 and co-funded under the European Regional Development Fund and by FutureNeuro industry partners, by the European Union's Horizon 2020 Research and Innovation Programme through the Marie Skłodowska-Curie under Grant Agreement No. 839553, by Armasuisse S+T with project CYD-C-2020003, by the University of Zürich UZH, and by the European Union Horizon 2020 Research and Innovation Program under grant agreement No. 830927, namely the H2020 Concordia Project.
Authors' addresses: S. L. Bernal and G. M. Perez, University of Murcia, Departamento de Ingeniería de la Información y las Comunicaciones, Murcia, Spain; emails: {slopez, gregorio}@um.es; A. H. Celdrán, Waterford Institute of Technology, Telecommunication Software and Systems Group, Waterford, Ireland and Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH, CH 8050 Zürich, Switzerland; email: ahuertas@tssg.org; M. T. Barros, University of Essex, School of Computer Science and Electronic Engineering, Essex, UK, Tampere University, CBIG/BioMediTech in the Faculty of Medicine and Health Technology, Tampere, Finland; email: michael.barros@tuni.fi; S. Balasubramaniam, Waterford Institute of Technology, Telecommunication Software and Systems Group, Waterford, Ireland, RCSI University of Medicine and Health Sciences, FutureNeuro, the SFI Research Centre for Chronic and Rare Neurological Diseases, Dublin, Ireland; email: sasib@tssg.org.

0360-0300/2020/12-ART11 $15.00
https://doi.org/10.1145/3427376

CCS Concepts: • **Security and privacy → Domain-specific security and privacy architectures**;

Additional Key Words and Phrases: Brain-computer interfaces, BCI, cybersecurity, privacy, safety

ACM Reference format:
Sergio López Bernal, Alberto Huertas Celdrán, Gregorio Martínez Pérez, Michael Taynnan Barros, and Sasitharan Balasubramaniam. 2020. Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. *ACM Comput. Surv.* 54, 1, Article 11 (December 2020), 35 pages.
https://doi.org/10.1145/3427376

1 INTRODUCTION

Brain-Computer Interfaces (BCI) emerged in the 1970s intending to acquire and process users' brain activity to perform later specific actions over external machines or devices [87]. After several decades of research, this functionality has been extended by enabling not only neural activity recording but also stimulation [167]. Figure 1 describes a simplification of the general components and processes defining a common BCI cycle in charge of recording and stimulating neurons [1, 26, 59], later presented in Section 2. It is important to note that these phases are not standard, so we include the most common ones used in the literature. The clockwise direction, indicated in blue, shows the process of acquiring neural data, and the counterclockwise represents the stimulation one, which is highlighted in red. Regarding the neural data acquisition, neurons interact with each other, producing neural activity, either based on previously agreed actions, such as controlling a joystick, or generated spontaneously (phase 1 of Figure 1). This activity is acquired by the BCI and transformed into digital data (phase 2). After that, data is analyzed by the BCI data processing system to infer the action intended by the user (phase 3). Finally, applications execute the intended action, enabling the control of external devices. These applications can present optional feedback to the users, which allows the generation of new neural activity. However, the counterclockwise direction of Figure 1 starts in phase 4, where applications define the intended stimulation actions to perform. Phase 3 processes this action to determine a firing pattern containing all the essential parameters required by the BCI to stimulate the brain. Finally, the firing pattern is sent to the BCI, which is in charge of stimulating specific neurons belonging to one or more brain regions and is dependent on the technology used. In a nutshell, a BCI can be a unidirectional or bidirectional communication system between the brain and external computational devices. Unidirectional communications are when they either acquire data or stimulate neurons, while bidirectional communications are when they perform both tasks [139].

From the security perspective, BCIs are in an early and immature stage. The literature has not considered security a critical aspect of BCIs until recent years, where terms such as neurosecurity, neuroprivacy, neuroconfidentiality, brain-hacking, or neuroethics have emerged [31, 58, 59]. Existing works of the literature have detected specific security attacks affecting BCI integrity, confidentiality, availability, and safety, but they do not perform a comprehensive analysis and miss relevant concerns [17, 87, 96, 163, 165]. More specifically, the use of neurostimulation BCIs in clinical environments introduces severe vulnerabilities that can have a significant impact on the user's health condition [136]. BCIs already existing on the market would benefit from the implementation of robust security solutions, reducing their impact, particularly in clinical environments. Furthermore, the expansion of BCIs to new markets, e.g., video games or entertainment, generates considerable risks in terms of data confidentiality [87, 96, 163, 165]. In this context, users' personal information, such as thoughts, emotions, sexual orientation, or religious beliefs, are under threats if security measures are not adopted [59, 96, 165]. Besides, contemporary BCI approaches, such as the use of silicon-based interfaces, introduce new security challenges due to the increase in the volume of acquired data and the use of potentially vulnerable technology [121]. The technological revolution

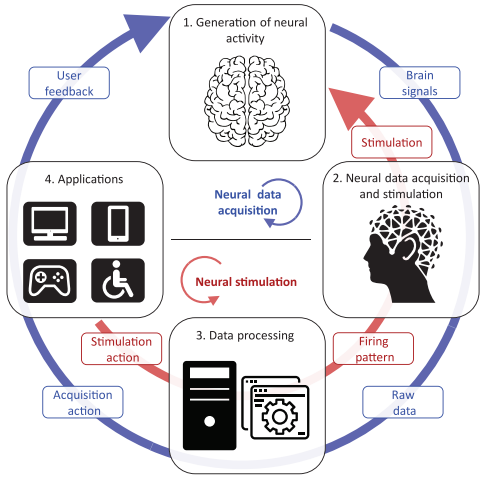

Fig. 1. General functioning of a bidirectional BCI. The clockwise flow indicated with a blue arrow represents the neural data acquisition process, while the counterclockwise flow represented with a red arrow models the brain stimulation.

of recent years, combined with movements such as the Internet of Things (IoT), brings an acceleration in the creation of new devices lacking security standards and solutions based on the concepts of *security-by-design* and *privacy-by-design* [17, 60, 137, 163, 165]. This revolution also brings to reality prospective and disruptive scenarios, where we highlight as examples the direct communications between brains, known as Brain-to-Brain (BtB) or Brainets [67, 126, 127, 184], and brains connected to the Internet (Brain-to-Internet (BtI)), which will require significant efforts from the security prism.

Once summarized the functioning of BCIs and their security status, the scope of this article lies in analyzing the security issues of software components that intervene in the processes, working phases, and communications of BCIs. Besides, this work considers the security concerns of infrastructures, such as computers, smartphones, and cloud platforms, where different BCI architectures are deployed. It is also important to note that, despite this article indicates overall impacts over the brain and the user's physical safety, the main focus of this work is to perform a security analysis from a technological point of view. Aligned with these aspects, and to the best of our knowledge, this article is the first work that exhaustively reviews and analyses the BCI field from the security point of view. Since these aspects have not been studied in depth before and BCI technologies are still immature, this line of work has a particular interest in a medium to long term. However, this area of knowledge is relevant nowadays, since devices already available on the market need to be protected against attacks.

In this context, Section 2 focuses on analyzing the security issues related to the design of the BCI life-cycle. We unify the existing heterogeneous BCI life-cycles in a novel and common approach that integrates recording and stimulation processes. Once proposed the new life-cycle design approach, we review the attacks applicable to each phase of the cycle, the impact generated by the attacks and the countermeasures to mitigate them, both documented in the literature and detected by us. After highlighting the security issues related to the BCI design, Section 3 reviews the inherent cyberattacks, impacts, and countermeasures affecting current BCI deployments scenarios. This section identifies the security issues generated by the devices implementing each life-cycle phase's responsibilities, as well as the communication mechanisms and the application scenarios. The last main contribution of this article is Section 4, where we give our vision regarding the trend

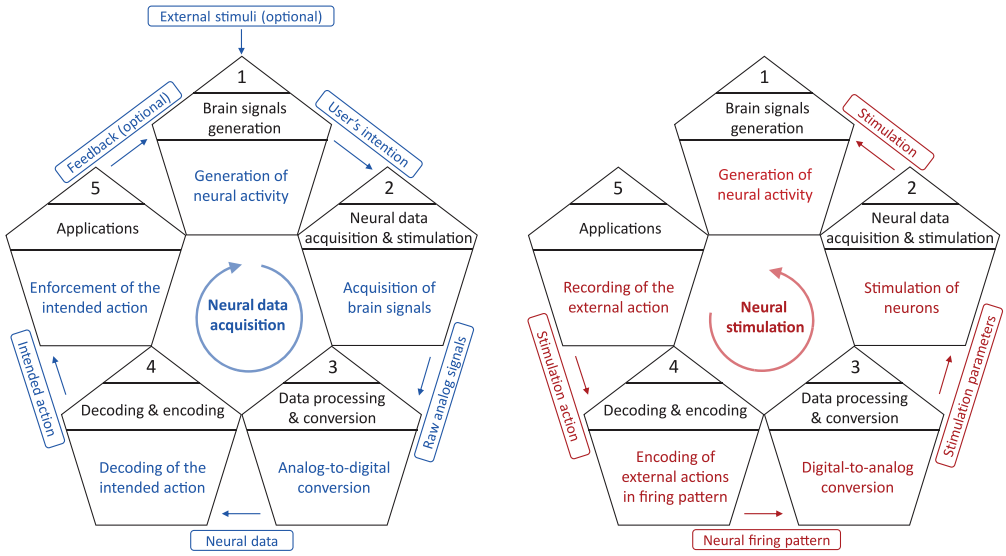

Fig. 2. Bidirectional BCI functioning cycle representing, in black, the common phases for neural data acquisition and brain stimulation. (Left side) Representation, in blue, of the processes performed and the data transferred by each phase of the neural data acquisition process. This cycle can be seen as a closed-loop process, because it starts and ends at the same phase. (Right side) Representation, in red, of the processes and transitions of each phase making up the stimulation process.

of BCI and the security challenges that this evolution will generate in the future. Finally, Section 5 presents some conclusions and future work.

2 CYBERATTACKS AFFECTING THE BCI CYCLE, IMPACTS, AND COUNTERMEASURES

This section reviews the different operational phases of BCIs detected in the literature, known as the BCI cycle, and homogenizes them in a new approach shown in Figure 2. After that, we survey the security attacks affecting each phase of the cycle, their impacts, and the countermeasures documented in the literature. We present as well unexplored opportunities in terms of cyberattacks, and countermeasures affecting each phase.

The literature has proposed different configurations of the BCI cycle. However, the existing versions only consider the signal acquisition process, missing the stimulation of neurons. These solutions present various classifications of the BCI cycle, as some do not consider the generation of brain signals as a phase, or group several phases in only one, without providing information about their roles [26, 59]. Other solutions, as proposed in References [6, 59, 87, 172], are confusing due to they define as new phases, transitions, and data exchanged between different stages. In terms of applications, some authors define a generic stage of applications [1, 26, 87, 148] while others deal with the concept of *commands* sent to external devices [10, 17, 18, 25, 54, 163, 171]. Also, just a few works define the feedback sent by applications to users [10, 17, 18, 25, 59, 87, 163, 171, 172]. To homogenize the BCI cycle and address the previously missing or confusing points, we present a new version of the BCI cycle with five phases (with clearly defined tasks, inputs, and outputs) that consider both acquisition and stimulation capabilities. Figure 2 represents our proposal, where the clockwise direction corresponds to the brain signal acquisition process. The information and tasks concerning this functioning are indicated in blue. In contrast, the stimulation process is indicated

in the counterclockwise direction, starting from phase 5, and, in each phase, the information and tasks are identified in red.

According to the neural acquisition process (clockwise direction in Figure 2), phase 1 focuses on the generation of brain signals. Generated data contain the user's intention to perform particular tasks; for example, controlling an external device. This phase can be influenced by external stimuli, producing modifications in the regular neural activity. In phase 2, the brain waves are captured by electrodes using a wide variety of technologies, such as Electroencephalography (EEG) or Functional Magnetic Resonance Imaging (fMRI). Raw analog signals containing the user's intention are then transmitted to phase 3, where data processing and conversion are required. In particular, this phase performs an analog-to-digital conversion procedure to allow further processing of the data. One of the main goals of this phase is to maximize the Signal-to-Noise Ratio (SNR), which compares the level of the target signal to background noise level to obtain the original signal as accurately as possible. Phase 4 processes the digital neural data to decode the user's intended action, where relevant features are calculated and selected from the neural data. After that, different models (e.g., classifiers, predictors, regressors) or rule-based systems determine the intended action [25, 148]. The action finally arrives at applications in phase 5, which execute the action. Applications can also send optional feedback to the user to generate brain signals and thus new iterations of the cycle.

Regarding the stimulation process (counterclockwise direction in Figure 2), the loop starts in phase 5, where it is specified the stimulation action in a general way (e.g., stimulate a particular brain region to treat Alzheimer's disease). This intended action is transmitted to phase 4, where this input is processed by different techniques, such as Machine Learning (ML), to generate a firing pattern that contains high-level information about the stimulation devices to be activated, the frequencies used and the temporal planning. Phase 3 intends to transform the firing pattern received, indicated in a general fashion, to specific parameters related to the BCI technology used. For example, the identification of neurons to stimulate or the power and voltage required for the process. Phase 2 transmits these stimulation parameters to the stimulation system, that is in charge of the physical stimulation of the brain. After this process, the brain generates neural activity as a response, which can also be acquired by the BCI to measure the state of the brain after each stimulation process. At this point, an alternation between brain stimulation and signal acquisition is possible, moving from one direction of Figure 2 to the other.

Before reviewing the attacks, impacts and countermeasures of each phase of the BCI cycle, it is essential to accurately define the concept of *security*, which refers to the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality and availability" [149]. The concepts of integrity, confidentiality and availability, together with the concept of *safety*, are used in this section as metrics to evaluate the impact of security attacks against BCI systems. The standard definitions of these concepts are the following:

- **Integrity:** "protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination" [76].
- **Confidentiality:** "preservation of authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information" [149].
- **Availability:** "property that data or information is accessible and usable upon demand by an authorized person" [149].
- **Safety:** "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment" [143]. This work considers the safety concept from the physiological, psychiatric, and psychological perspectives.

Table 1. Definition of the Attacks Detected for the BCI Cycle

Attack	Description
Adversarial attacks [38, 90]	Presentation of intentionally crafted inputs to an ML system to disrupt its normal functioning and output.
Misleading stimuli attacks [40, 79, 96]	Presentation of malicious sensory or motor stimuli to users aiming to generate a specific neural response.
Buffer Overflow attacks [16, 109, 147]	Access to out-of-bounds memory spaces due to insecure software implementations. They take advantage of operations over memory buffers whose boundaries are not well managed.
Cryptographic attacks [58, 59]	Exploit vulnerabilities in the elements that define a system, such as algorithms, protocols or tools. A variety of techniques focused on evading the security measures of cryptographic systems.
Firmware attacks [13, 173]	Extract or modify the firmware of a device, a critical piece of software that controls its hardware.
Battery drain attacks [24, 135]	Consume the battery of a device, reducing its performance or even making it permanently inaccessible.
Injection attacks [105, 134]	Present an input to an interpreter containing particular elements that can modify how it is parsed, taking advantage of a lack of verification of the input.
Malware attacks [77, 154, 177]	Use of hardware, software or firmware aiming to gain access over computational devices to perform malicious actions intentionally.
Ransomware attacks [2, 37]	Encrypt users' data and demand later an economic ransom to decipher it.
Botnet attacks [4, 92]	Use of botnets, networks of infected devices controlled and coordinated by an attacker, to perform particular attacks directed to specific targets.
Sniffing attacks [5]	Acquisition of private information by listening to a communication channel. When the data is not encrypted, attackers have access to the content of the whole communication.
Man-in-the-middle attacks [163]	Alteration of the communication between two entities, making the extremes believe that they are communicating directly between each other.
Replay attacks [77, 166]	Retransmission of previously acquired data to perform a malicious action, such as the impersonation of one of the legitimate participants of the communication.
Social engineering attacks [47, 49]	Psychological manipulation to gain access over restricted resources. An example is phishing attacks, based on the impersonation of a legitimate entity in digital communication.
Spoofing attacks [159, 166]	Masquerade an entity of the communication, transmitting malicious data. Frequent spoofing attacks in network communications are, among others, IP spoofing and MAC spoofing.

At this point, it is essential to note that in this document, the safety concept refers to the preservation of the physical integrity of BCI users, not focusing on the conservation of objects or the environment. To better understand the attacks and countermeasures later discussed in this section, Table 1 offers a brief description of the attacks affecting BCI, whereas Table 2 describes their countermeasures. For each phase of the BCI cycle, we detail the particularities of these attacks and countermeasures.

Figure 3 indicates the attacks, impacts, and countermeasures described in this section. As can be seen, each attack is represented by a color that associates the impacts it generates and the countermeasures to mitigate it. For each impact included in the figure, it includes a simplified version of the BCI cycle. Those phases of the cycle marked in red indicate impacts detected in the literature for that specific phase, whereas the blue color indicates our contribution. Besides, the attacks, impacts and countermeasures marked with references have been proposed in the literature, while those without references are our contribution. It is important to note that this figure highlights the limitations exposed by the literature, as can be appreciated by the volume of our contributions. To simplify the image, we have synthesized most of the safety impacts into a general entry "Cause physical damage," describing the specific impacts over users' health in detail throughout the section.

Table 2. Definition of the Countermeasures Detected for the BCI Cycle

Countermeasure	Description
Training sessions, demos and serious games [59]	Initiatives to increase the awareness of the users about the risks of technology.
User notifications [24]	Alert the users in case an attack is detected, to take part in the defence (e.g., stop using the device).
Directional antennas [186]	Antennas that radiate or receive the energy mainly in particular directions, aiming to reduce interference.
Analysis of the medium [59]	Sensing of the communication medium to detect abnormal behavior.
Low transmission power [170]	Reduction of transmission power to avoid the interception of the communication by malicious entities.
Frequency and channel hopping [46, 186]	Wireless communication models based on pseudo-random hopping patterns previously known by sender and receiver.
Spread spectrum [166, 170, 186]	Transmission of the information in a broader bandwidth to avoid interference in the wireless medium.
Access control mechanisms [24, 164, 165]	Means of detecting and preventing unauthorized access to particular resources.
Privilege management [110–112]	Assign privileges to different groups of users based on roles.
Whitelists and blacklists [106]	List of entities, such as systems or users, that are allowed or forbidden, respectively, to perform specific actions.
Cryptographic mechanisms [8]	Use of encryption and decryption techniques to protect the privacy of data, since unprotected information can be accessed and modified by attackers.
Differential privacy [60, 90]	Cryptographic mechanism based on the addition of noise to the data aiming to suppress sensitive aspects, accessible when combined with a large amount of a user's data.
Homomorphic encryption [90]	Cryptographic mechanism allowing the computation of mathematical operations over ciphered data, generating an encrypted result.
Functional encryption [164, 165]	Cryptographic mechanism where having a secret key allows to learn a function of encrypted data without revealing the data itself.
Authenticity verification [8]	Ensure that the data we are accessing, or the endpoint we are communicating, is who it claims to be.
Legitimacy verification [8]	Review if a malicious software application has replaced a legitimate one.
Feature limitation [123]	Ensure that any software only implements the specific functionality for which it was intended.
Periodic updates [37]	Correct detected vulnerabilities and include new functionalities to reinforce the existing countermeasures.
Robust programming languages [110]	Choose the most adequate languages taking into consideration their strengths and weaknesses.
Compilation techniques and options [111]	Specific capabilities of compilers to protect out of bounds accesses to the device memory or CPU registers.
Application hardening [50]	Modification of an application to make it more resistant against attacks, such as the obfuscation of the application code.
Segmented application architectures [147]	Isolation of architectures and systems, establishing different containers and security groups to communicate with each other.
Sandboxing [104]	Isolate the execution of different programs, allowing its protection against attacks.
Antivirus [159]	Software focused on the prevention, detection, and elimination of malware attacks. Modern antivirus offer protection for a wide variety of threats.
Malware visualization [41]	Technique focused on the analysis of software binaries in a graphical way to detect anomalous malware patterns.

(Continued)

Table 2. Continued

Countermeasure	Description
Quarantine of devices [4]	Isolation of infected or potentially infected software, to avoid further propagation and infection.
Backup plans [3]	Recurrent copy of data stored in a different location to allow its recovery in case of data loss.
Defense distillation [90]	Creation of a second ML model based on the original, with less sensitivity regarding input perturbations and offering smoother and more general results.
Data sanitisation [66]	Rejection of samples that can produce a negative impact on the model, preprocessing and validating all input containing adversarial information.
Adversarial training [44]	Inclusion of adversarial samples in the training process to allow the recognition of attacks in the future.
Monitoring systems [15]	Capture and analyze the behavior of the entities within a system and their communications.
Anomaly detection [24]	Detection of odd behaviors on systems that can potentially correspond to an attack situation.
Firewall [159]	Cybersecurity system that only allows incoming or outgoing network communications previously authorized.
IDS [159]	Analysis of the network activity to identify potentially damaging communications aiming to disrupt the system.
Communication interruption [73]	Detention of an active communication to mitigate the impact of an attack if there is evidence of its presence.
Input validation [134]	Analysis and preprocessing of inputs presented to a system to suppress potential causes of failure.
Randomization [165]	Change of existing data in a way that does not follow a deterministic pattern and prevents privacy leakage.
BCI Anonymizer [17]	Anonymization of brain signals acquired from the brain to be shared without exposing users sensitive information.

2.1 Phase 1. Brain Signals Generation

2.1.1 Attacks. Considering the neural data acquisition flow, this first phase focuses on the brain processes that generate neural activity, which can be influenced by external stimuli. The literature has detected *misleading stimuli attacks* [40, 79, 96], a mechanism to alter the brain signals generation by presenting intentionally crafted stimuli to BCI users. To understand these attacks, it is important to introduce some concepts. *Event-related Potentials (ERP)* are neurophysiological responses to a cognitive, sensory, or motor stimulus, detected as a pattern of voltage variation [26]. Within the different types of Event-related Potentials (ERPs), Evoked Potentials (EP) focus on sensory stimuli and can be divided into two categories, Visual Evoked Potentials (VEPs) and Auditory Evoked Potentials (AEPs), related, respectively, with visual and auditory external stimuli. Specifically, *P300* is a Visual Evoked Potential (VEP) detected as an amplitude peak in the Electroencephalography (EEG) signal about 300ms after a stimulus, extensively used due to its quick response [158].

On the one hand, Martinovic et al. [96] used the P300 potential to obtain private information from test subjects and demonstrated misleading stimuli attacks. Visual stimuli were presented in the form of images, grouped as follows: four-digit PIN codes, bank ATMs and credit cards, the month of birth, and photos of people. The objective of the experiment was to prove that users generate a higher peak in the P300 potential when faced with a known stimulus and, therefore, be able to extract private information. The authors used the Emotiv EPOC 14-channel headset [36], a commercial BCI EEG device, showing that information leakage, measured in information entropy, was 10%–20% of the overall information, and could be increased to approximately 43%. On the other hand, Frank et al. [40] demonstrated the possibility of performing subliminal *misleading*

stimuli attacks. To perform the experiments, the same ERP concept with P300 potentials was used. In this work, the authors showed information hidden within the visual content projected to 29 subjects, in the form of stimuli with a duration of 13.3 milliseconds, imperceptible to the human eye. The study used EEG devices of the brands NeuroSky [118] and Emotiv [34]. We consider that the previous works are relevant to highlight the importance of security in BCI, and additional experiments with a higher number of users are required.

The literature has documented some well-known methods to present stimuli to users and analyze their neural responses [17, 96, 163]. For example, to study the neural activity generated after a question in a lie detection test [79]. Although these methods do not represent attacks themselves, they are an opportunity to develop new misleading stimuli attacks against BCIs, defined as follows:

- *Oddball Paradigm*: specific target stimuli, hidden between a sequence of common non-target stimuli, would generate peaks in ERP. For example, to differentiate a known face among several unknown ones.
- *Guilty Knowledge Test*: the response generated by familiar stimuli can be differentiated from the generated by unfamiliar elements. This principle has been used for lie detection.
- *Priming*: a stimulus can generate an implicit memory effect that later influences other stimuli.

Despite the comprehensive study in the literature on Auditory Evoked Potentials (AEPs), there are no specific works, to the best of our knowledge, describing attacks over auditory stimuli. However, Fukushima et al. [42] described that inaudible high-frequency sounds could affect brain activity. We detect that this scenario generates new opportunities for attackers, since the generation of inaudible auditory stimuli does not require close interaction with the victim, helping the attacker to remain undetected.

Regarding neural stimulation, this phase represents the result of the stimulation process within the brain. Based on a lack of literature defining taxonomies of attacks over the brain, we identify two main attack categories during neurostimulation. The first category consists of taking control of the stimulation process to cause neural tissue damage. These attacks may reproduce or worsen the secondary effects often present during the treatment of neurological conditions, such as Parkinson's disease, either by over-stimulation actions or by preventing the treatment. The feasibility of these attacks is supported by References [48, 128], who indicated that the adverse effects of neurostimulation are related to the parameters and patterns of the stimulation. Additionally, we identify another modality of attack in this category, based on recreating known neurological conditions if there is an existing neurostimulation device with access to the regions naturally affected by those diseases. As an example, we identify the possibility of recreating neurodegenerative diseases, such as Parkinson's and Alzheimer's diseases, based on a deterioration of cerebral tissue, and epileptic seizures. Although these attacks are nowadays just theoretical [11], the advance of prospecting BCI technologies like Neuralink [116], could result in neurostimulation systems that can cover various parts of the brain, thus introducing these threats.

The second category of attacks focuses on inducing an effect or perception in the user. It is well known that neurostimulation can cause multiple psychiatric and psychological impacts, such as mood variations, depression, anxiety, or suicidal thoughts, as later indicated in Section 2.1.2. An attacker could magnify these effects with malicious stimulation parameters to take advantage of the user. As an example, the attack could aim to reduce the patient's inhibition to ease the extraction of private information. This situation introduces the possibility of *social engineering attacks* to BCI, where the attacker would not require sophisticated social techniques to manipulate its victims psychologically.

Table 3. Summary of the Most Common Side Effects During FDA-approved Neurostimulation

Technology	Condition	Brain region	Neurological side effects	Psychiatric/psychological side effects
DBS	Parkinson's disease	STN	Akinesia, cramping in the face or hand, dysarthria, dysphagia, eyelid apraxia, gait disturbance, hypersalivation, impaired vision, incontinence, learning and memory difficulties, paresthesia, postural instability, speech disturbance, lack of verbal fluency, vegetative symptoms, weakness [23, 30, 33, 48, 157]	Anxiety, apathy, cognitive disturbance, confusion, depression, hallucination, submanic state [23, 33, 48]
		GPI	Similar to STN [48]	Anxiety, depression, suicidal thoughts [33, 48]
		VIM	Dysphagia, fine motor disturbance, speech disturbance [157]	
	Essential tremor	VIM	Dysaesthesia, dysarthria, gait disturbance, paresthesia, speech disturbance [23, 33]	
	Dystonia	GPI	Gait disturbance, paresis, speech disturbance, tetanic muscle contractions, visual deficits [23, 33]	Anxiety, cognitive disturbance, confusion, hallucination [23]
	Obsessive-compulsive disorder	VC/VS, NAc		Depression, operant conditioning, reward processing alteration, suicidal thoughts, suicide [102]
RNS	Epilepsy	Seizure origin	Death, change in seizures, hemorrhage, infection [117]	Anxiety, depression, suicide, suicididal thoughts [117]

2.1.2 Impacts. It is important to note that the *misleading stimuli attacks* detailed for this phase have only been conducted against data confidentiality [40, 79], aiming to extract sensitive data from BCI users. However, we consider that they can also affect BCI integrity, availability, and safety. These stimuli can alter the normal functioning of this phase, generating malicious inputs for the next stages that can derive on disruptions of the service or incorrect actions aiming to cause physical damage to users. Specifically, Landau et al. [79] identified that misleading stimuli attacks performed during a medical diagnose, such as a photosensitive epilepsy test in which different visual stimuli are presented, can derive in a misdiagnosis, affecting the users' safety. We also identify as feasible that malicious stimuli, both perceptible or subliminal, can affect the users' mood.

From the perspective of neurostimulation, the attacks above can affect users' health differently according to their previously existing diseases, impacting their physical and psychological safety. The issues related to different BCI technologies are detailed in Section 2.2, indicating general impacts over the brain in this phase. Table 3 presents the most common side effects during particular neurostimulation therapies. As can be seen, performing an attack during the stimulation process can aggravate or even generate a wide range of negative impacts on BCI patients. Additionally, the authors of References [135, 136] highlighted common issues to neurological diseases, such as tissue damage, rebound effects, and denial of stimulation (also affecting the service availability). Besides, they identified that an alteration of voltage, frequency, pulse width, or electrode contact used to stimulate the brain could modify the volume of cerebral tissue activated, inducing non-desired effects in the surrounding structures depending on the electrode location and stimulation technique. Pycroft et al. [135] also indicated that an attack on neurostimulation could induce a patient's thoughts and behavior. In Reference [95], the authors highlighted that attacks on neurostimulation can prevent patients from speaking or moving, cause brain damage or even threaten their life, while the authors of Reference [79] indicated the user's frustration if the result of the process is not adequate.

Pycroft et al. [136] indicated potential attacks and harms against neurostimulation patients. First, they detected that an overstimulation procedure could cause tissue damage, independently of the type of stimulation and medical condition. For Parkinson's disease, an attacker could apply

a ~10Hz stimulation over the STN region to produce hypokinesia or akinesia. In patients with essential tremor, where the ventral intermediate nucleus (VIM) is stimulated, both an increase of voltage and a decrease of frequency could dangerously derive in exacerbated tremor. Finally, a variation in the stimulation parameters during the treatment of obsessive-compulsive disorder could generate alterations of reward processing or operant conditioning.

Based on the above, safety impacts are the most damaging in this phase, presenting a risk of irreversible physical and psychiatric issues. In addition, taking advantage of the victim's psychological status, it could ease social engineering attacks as well. The attacker could aim to reduce or inhibit the patient's mental defense mechanisms, acquiring sensitive information, thus impacting data confidentiality. However, more worrisome would be to take advantage of the victim's mental status, in which the patient unconsciously accedes to undesired acts, such as gambling money, buying unnecessary products, committing a crime, or participating in non-consensual sexual intercourse.

2.1.3 Countermeasures. Focusing on the countermeasures to mitigate misleading stimuli attacks, multiple works [24, 79, 135, 136] identified general measures to raise the awareness of BCI users, such as spreading the risks of these technologies among clinicians and patients and the education of the users in these technologies. This is especially interesting, since humans usually are the weakest element of a security system. In particular, Ienca et al. [59] indicated that specific training sessions could be beneficial to protect users against potentially unsafe stimuli related to authentication methods and banking-related information. Besides, the inclusion of demos and serious games in commercial BCI devices may educate them on the risks of these technologies. However, these countermeasures can only be applied when the user is aware of the stimuli. Because of that, we consider that *misleading stimuli attacks* can be reduced if BCIs are complemented with external systems that monitor the stimuli presented and give users the possibility to evaluate if the content is appropriate. For example, by analyzing if the multimedia contents showed to users, such as images or videos, have been maliciously modified [15, 175], even if they are subliminal. Additionally, we propose using predictive models based on anomaly detection systems, aiming to detect an attack in its early stage and deploy mechanisms to mitigate them.

2.2 Phase 2. Neural Data Acquisition and Stimulation

2.2.1 Attacks. This second phase focuses on the interaction of BCI devices with the brain to acquire neural data or perform its stimulation. Regarding data acquisition, the authors of References [79, 87] identified the use of a combination of *replay and spoofing attacks* in which previous signals from the BCI user, signals from other users, or synthetic signals can impersonate the legitimate brain waves. We detect the applicability of these attacks to stimulation systems, where an attacker can force specific stimulation behaviors based on previous actions. One possible outcome of this control can be an increase in the voltage delivered to the patient's brain [95]. Besides, the authors of References [59, 79] detected the use of *jamming attacks* against the neural data acquisition process, transmitting electromagnetic noise to the medium. Based on Vadlamani et al. [170], we also identify this problem in neural stimulation, where *jamming attacks* can override the legitimate signals emitted by the BCI electrodes if they are transmitted with enough power.

2.2.2 Impacts. Regarding the impacts produced by the previous attacks, Li et al. [87] identified that *replay and spoofing attacks* affect both data integrity and availability, being able to disrupt the acquisition process. Landau et al. [79] highlighted that these attacks could interfere with clinical diagnosis procedures, replacing the legitimate brain signals by malicious ones, concluding in misdiagnosis, and producing either an absence of treatment or an unnecessary one on healthy patients. We identify that these attacks, applied to the stimulation scenario, can disrupt the

stimulation process or acquire and modify the stimulation pattern used by the BCI to maliciously stimulate the neurons, affecting data integrity, data and service availability, and the patient's safety. Focusing on *jamming attacks*, an attacker can aim to prevent the electrodes from capturing brain signals due to the noise transmitted [59, 79], affecting their availability and safety. We detect that jamming attacks can also affect neurostimulation scenarios, where signals with enough power can override the legitimate ones, affecting the integrity and availability of the data, as well as the patient's safety during stimulation actions.

Apart from the impacts derived from the previous attacks, it is important to note that each specific BCI technology presents specific risks according to their invasiveness and functioning, and thus the impact generated by an attack differs. To analyze this situation, we select some of the most used BCI technologies used to acquire neural data or stimulate the brain. For each one of them, we address specific considerations to evaluate their impact.

Regarding the issues related to acquisition technologies, it is necessary to consider both their temporal and spatial resolutions. We identify that a low temporal resolution in acquisition technologies presents concerns on data and service availability, since the devices transmit a reduced amount of data that can be affected more easily by electromagnetic interference and, especially, *jamming attacks*. Besides, this situation can also be beneficial for *replay and spoofing attacks*, since attackers have more time to prepare and send malicious data. A high spatial resolution can impact on data confidentiality, allowing attackers to have access to more sensitive neural data. It is worthy to note that attacks on technologies such as Functional Magnetic Resonance Imaging (fMRI) or Magnetoencephalography (MEG) can potentially have a higher economic impact due to the high cost of these technologies compared to others like EEG [82, 137]. Nevertheless, EEG is the most studied acquisition technology from the security perspective, due to its wide availability outside clinical environments, highlighting the feasibility of attacks such as *misleading stimuli attacks* or *jamming attacks*.

Although the literature has documented some potential security impacts for acquisition technologies, the impact of neurostimulation technologies on patient's health has been studied in a more detailed way, specifically in the field of Implantable Medical Devices (IMDs). Because of that, we first introduce the most common stimulation technologies nowadays to review their specific impact later, mainly addressing safety issues.

Focusing on the specific impacts of neurostimulation technologies, Deep Brain Stimulation (DBS) is the most studied one due to its invasiveness, where Medtronic is one of the most popular brands commercializing open-loop DBS devices [128]. The side effects of this method have been extensively studied in the literature, where some of them have previously been presented in Table 3 for the treatment of particular conditions. According to Pycroft et al. [136], the use of Deep Brain Stimulation (DBS) with high charge densities can cause tissue damage. Furthermore, an increase or decrease in the stimulation frequency can have a considerable impact on its efficacy, even reversing the stimulation effect. Finally, an alteration of emotion and affect processing can occur during DBS as side-effects, such as pathological crying or inappropriate laughter, having a distressing impact.

Moving to Transcranial Magnetic Stimulation (TMS), Polanía et al. [129] indicated that pulses applied to particular areas could induce suppression of visual perception or speech arrest, which serves as an opportunity for attackers. León et al. [84] highlighted that Transcranial Magnetic Stimulation (TMS) could produce side-effects such as headache and neck pain, being epileptic seizures possible but improbable. The side effects of Transcranial Electrical Stimulation (tES) usually are mild, such as skin tingling, itching, and redness [114]. Nevertheless, this technique can have indirect effects on the stimulation of non-neuronal elements, such as peripheral nerves, cranial nerves, or retina. Because of that, the stimulation is limited to maximum tolerable doses [89].

Besides, in patients with depression, Direct Current Stimulation (tDCS) can derive to mania and hypomania cases [99]. It is worthy to note that the side effects described above can naturally arise in controlled environments where clinicians have strict control over the procedure. However, if attackers alter the therapy, they could recreate or amplify malicious conditions, generating a clear impact on patients' health.

The Neuropace RNS is a closed-loop neurostimulation system for treating drug-resistant epilepsy, performing both neural data acquisition and neurostimulation procedures. It presents the advantage of delivering stimulation only when detecting the beginning of seizure activity, reducing secondary effects. Nevertheless, it introduces potential challenges than can be used by an attacker to impact its users' safety [128]. First, we identify that the closed-loop behavior could induce, in both clinicians and patients, a reduction of the perception of risks, assuming that the device is working correctly. Furthermore, since the device presents autonomous capabilities, an attacker could disrupt its behavior, without the knowledge of the user, to generate an impact on data confidentiality, service availability, and safety.

2.2.3 Countermeasures. Regarding the countermeasures to detect and mitigate replay and spoofing attacks, Landau et al. [79] proposed, for data acquisition, the use of anomaly detection mechanisms to detect modified inputs, as well as the accuracy improvement of acquisition devices. Besides, we propose a mechanism able to disable the electrodes not required for the current application usage and avoid potential risks, such as the acquisition of P300 in brain signals. This action could be performed automatically by the BCI system or based on the patient's or clinician's decision. Taking into account neural stimulation, and specifically for IMDs, external devices to authenticate and authorize the stimulation actions can be used [24]. The authors of References [46, 170, 186] documented several detection mechanisms and countermeasures related to the mitigation of jamming attacks. All detection procedures are based on an analysis of the medium to detect abnormal behavior, as identified for neural data acquisition by Ienca et al. [59]. Specifically, Landau et al. [79] proposed using an ensemble of classifiers to detect the addition of noise to the benign input. As proposed countermeasures, Vadlamani et al. [170] identified the use of low transmission power as a possible solution to harden the detection of the legitimate transmission, and the use of directional antennas oriented to the brain to avoid the jamming. The use of frequency hopping [186] and channel hopping [46] after a particular duration of time also aim to reduce the impact of these attacks. We detect that the use of directional antennas is also a possible solution for *replay and spoofing attacks*. Finally, it is worthy to note that the mitigation of the previous impacts focused on user's safety is the consequence of mitigating the attacks spotted against BCI devices.

In the scenario of closed-loop neurostimulation systems, we identify as essential to have information about the behavior of the device, from both acquisition and stimulation procedures. These feedback mechanisms would allow to externally analyze the status of the brain and the stimulation decisions. Another proposal is the use of anomaly detection systems, included in the device, to identify unusual stimulation parameters, or an absence of treatment when a seizure occurs, notifying the user. This second approach could be more energy preserving, and the election of the strategy would depend on the use case.

2.3 Phase 3. Data Processing and Conversion

2.3.1 Attacks. This phase performs the data processing and conversion tasks required to allow neural data and stimulation actions to be ready for subsequent stages. Although the literature has not detected security problems in this phase, according to the aspects indicated by Bonaci et al. in References [17, 18], we identify *malware attacks* as possible against this phase, taking control over the BCI. These attacks are candidates to affect both acquisition and stimulation processes,

impacting the tasks performed in this phase. In particular, we identify that malware can disrupt the analog-to-digital conversion that occurs during neural data acquisition, as well as the translation of firing patterns to particular stimulation devices. We also detect that *jamming attacks* applied to the previous phase for data acquisition can impact this phase, since a distorted input signal with enough noise can be difficult to filter and thus propagate this signal to subsequent phases.

2.3.2 Impacts. In this context, we identify that *malware attacks* have an impact on both neural data acquisition and stimulation, where attackers alter or override the data received from previous phases, generating malicious data sent to subsequent phases. That is, the analog data recorded during neural data acquisition or the firing pattern used in neurostimulation processes. These attacks can gather the sensitive data managed in this phase, both analog and digital, and send it to the attackers, affecting data confidentiality. For example, information about private thoughts or neurological treatments. In terms of data and service availability, both acquisition and stimulation are potentially vulnerable to malware that avoids data transmission to subsequent phases of the cycle. Malware affecting integrity and availability is also a threat against users' physical safety, generating damaging stimulation patterns or dangerous actions sent to applications. Besides, the impacts and countermeasures described in the first phase of the acquisition flow for jamming attacks are also applicable to the current stage.

2.3.3 Countermeasures. Regarding the countermeasures to mitigate attacks affecting data confidentiality, Chizeck et al. [26] defined a U.S. patent application entitled "Brain-Computer Interface Anonymize" that proposes a technology capable of processing neural signals to eliminate all non-essential private information [17, 165]. As a result, sensitive information is never stored in the BCI device or transmitted outside. We identify this method as especially relevant in this phase, as it is the first stage after the BCI's acquisition process. Although the authors do not provide details about techniques or algorithms to understand how raw signals are processed, they indicate that this process can only be performed on hardware or software within the device itself, and not on external networks or computer platforms, as a way to ensure the privacy of the information. Besides, Ienca et al. [60] proposed the use of *differential privacy* to improve the security and transparency of data processing.

The countermeasures to mitigate malware depend on their type and behavior. We consider the use of antivirus software and Intrusion Detection Systems (IDS) as alternatives for the protection of individual devices, based on Reference [79]. Besides, the authors of References [159, 177] considered perimeter security mechanisms, such as *firewalls*, responsible for analyzing all incoming and outgoing communication of the device. We also propose using Machine Learning (ML) anomaly detection systems to identify potential malware threats [24, 141]. Finally, Chakkaravarty et al. [154] reviewed current persistent malware techniques able to bypass common countermeasures and proposed mitigation techniques, such as *sandboxing* [104], *application hardening* [50], and *malware visualization* [41]. It is essential to highlight that the countermeasures applicable for this phase highly depend on the device constraints that implement this phase, which is typically the BCI device (see Section 3).

2.4 Phase 4. Decoding and Encoding

2.4.1 Attacks. Decoding and encoding is the phase focused on identifying the action intended by the users in neural data acquisition or the specification of the neural firing pattern in neurostimulation. *Malware* attacks have been identified in the literature by Bonaci et al. [17, 18] from the signal acquisition perspective. Specifically, they identified that attackers could use *malware* to either override the functioning of this phase or to implement additional malicious algorithms. Besides, we identify that *malware* attacks can also be applied to the stimulation flow, avoiding or

disrupting a firing pattern's generation. Besides, we identify that *adversarial attacks* can also be applied to this phase for both acquisition and stimulation tasks, taking advantage of the classification algorithms used. These attacks affect all types of ML models, and, because of that, they are currently an open challenge [38]. Liu et al. [90] detected the possibility of *poisoning attacks*, where attackers introduce crafted adversarial samples to the data, aiming to change its distribution. *Evasion attacks* aim to create samples that evade detection systems, whereas *impersonate attacks* focus on adversarial samples that derive in incorrect classification of the legitimate ones. Finally, two attack models exist according to the knowledge about the model [44]. In *white-box attacks*, adversaries know the model, while in *black-box attacks*, they only have access to the model through a limited interface.

2.4.2 Impacts. The previously described attacks generate particular impacts on BCI. On the one hand, *malware* has an impact on data integrity and availability, as it can alter or ignore the received data from previous phases, and override the output of the current one. That is, disrupt the intended action sent to BCI applications in the acquisition process, such as preventing the control of a wheelchair or changing its direction, or the firing pattern in neural stimulation, enabling a wide variety of attacks as described in Section 2.1. Besides, *malware* affects the availability of the ML process by the alteration of the trained model or the ML algorithm. From a data confidentiality perspective, *malware* can access the features used in the ML training phase, as well as gather information about the model and the algorithm used. *Malware* also affects users' safety, as the previous integrity and availability impacts derive in malicious actions and firing patterns that affect the integrity of users, such as causing neural damage or inducing particular psychological states. On the other hand, *adversarial attacks* also affect data integrity and availability, as the introduction of malicious samples aiming to disrupt the model can alter or avoid the generation of actions and firing patterns. Shokri et al. [153] demonstrated that ML models are sensitive against *adversarial attacks*, aiming to detect if a sample exists in the model's training dataset. Based on that, an attacker may extract sensitive users' data, such as previous intended actions or used patterns during stimulation actions. Taking into account data confidentiality, Landau et al. [79] detected that a malicious entity taking control of the output of this phase could access the user's intention. Finally, the use of malicious samples, as is the case of *poisoning attacks*, alter the ML system, deriving in safety impacts for both cycle directions.

2.4.3 Countermeasures. To mitigate the attacks on the ML training phase affecting integrity and availability, we have identified several techniques proposed in the literature for generic *adversarial attacks*, that can serve as an opportunity to improve the security of BCI. First, *data sanitization* is useful to reject samples containing adversarial information, thus disrupting the model. Jagielski et al. [66] proposed a similar approach against poisoning attacks applied to regression techniques, where noise and *outliers* are suppressed from the training dataset. Nevertheless, it does not prevent attackers from crafting samples similar to those generated by the legitimate distribution. Countermeasures such as *adversarial training* or *defense distillation* have been presented in this context. However, both have limitations, as they depend on the samples used during the training and can be broken using *black-box attacks* and computationally expensive attacks based on iterative optimization [44, 90]. Goodfellow et al. [44] also proposed *architecture modifications*, based on the improvement of ML models to be more robust, but this derives in models difficult to train that have degradation in the performance when used in non-adversarial situations. Liu et al. [90] documented the integration of techniques to mitigate the attacks, called *ensemble method*. They also indicated two methods that can apply in both training and testing phases: *differential privacy* and *homomorphic encryption* [56, 90, 165]. Finally, it is worthy to note that the countermeasures to mitigate *malware attacks* in the previous phase can apply to the current one.

2.5 Phase 5. Applications

2.5.1 Attacks. From the data acquisition context, applications perform in the physical world the actions intended by users through their neural activity. These actions can range from the interaction with a computer or smartphone, to the control of a robotic limb. From the perspective of neural stimulation, applications are the entry point of the information transmitted to the brain, like sensory stimuli in prosthesis or cognitive enhancement. In this section, we consider attacks on applications, without analyzing their communication with external systems, addressed in Section 3.1.

Considering the issues of this phase, *spoofing attacks* over BCIs have been detected in the literature, where an attacker creates malicious applications identical to the original and make them available in app stores [8]. The authors of References [17, 18, 87] identified *malware attacks* as a threat in BCI. Besides, Pycroft et al. [136] identified that the use of consumer devices, such as smartphones, generates new risks and security problems. Specific considerations about malware are the same as detailed in Sections 2.3 and 2.4. Moreover, we have found several opportunities related to cyberattacks performed against applications. In particular, we detect security misconfiguration issues, Buffer Overflow (BO) attacks, and injection attacks over applications. However, the detailed analysis of these particular attacks is out of the scope of this work, and we only address general aspects related to BCI.

2.5.2 Impacts. Landau et al. [79] identified multiple risks on BCI applications with the independence of any attack. They detected that an attacker could interfere with the user's ability to use the device, impacting its availability. They also detected confidentiality concerns regarding the identification of users by their neural data, illustrating a scenario in which an attacker extracts EEG data from the application and compares it with the EEG database of a hospital, identifying the user and accessing his or her medical records. This identification can derive in a discrimination situation based on the belonging of specific groups, such as religious beliefs. Besides, most BCI development APIs offer full access over the information and do not implement limitations on the stimuli presented to users, generating confidentiality issues [17, 40, 87, 96, 163, 165]. Finally, all the attacks affecting this phase can force applications to send malicious stimuli or actions, causing physical harm [8].

Considering the impact of the previous attacks, applications created by *spoofing attacks* affect both data integrity and confidentiality, as they can present malicious stimuli to obtain sensitive neural information, such as thoughts or beliefs [8]. In neurostimulation scenarios, we identify that these fraudulent applications could entirely modify the firing patterns used to stimulate the patient, generating a high impact over safety. More particularly, these applications could induce psychological states in the victim, making them more willing to gamble, or even generate adverse effects such as anxiety and depression. Based on that, the attacker could take advantage of these mental states, injecting in-app advertisements to earn money from the victim.

Malware attacks impact the integrity of the applications by altering their services and capabilities, such as disabling the encryption of information. Besides, they can compromise applications' confidentiality, gaining access to sensitive information such as medical records and user profiles used during neurostimulation treatments. Concerning the availability of the application, *malware attacks* can derive in denial of service over the application, impacting in processes such as controlling prosthetic limbs or wheelchairs.

We detect that *misconfiguration attacks* present data integrity issues, where attackers take advantage of the system to gain unauthorized access, such as weak access control mechanisms. Data confidentiality issues are also present, for example, on configuration files that have static predefined passwords, allowing attackers to gain access to users' private data. Applications' availability

problems are also possible, as a misconfiguration issue can serve as a first step to disrupt the normal behavior of the BCI application.

Moving to *injection attacks*, they can produce data loss, modification, and corruption, affecting the integrity of applications [105, 134]. In terms of confidentiality, they can produce the disclosure of sensitive information to unauthorized parties [105, 134], such as insurance companies aiming to select the best candidates for their products [8]. Availability can be affected by a denial of access over an authentication system, or producing crash, exit or restart actions on the applications, disrupting vital processes such as clinical neurostimulation [107, 134].

Buffer Overflow (BO) attacks can derive in the execution of unauthorized code or commands, where an attacker can alter the normal functioning of the application or access to sensitive information [110]. Furthermore, they can also aim to bypass protection mechanisms by the execution of code outside the scope of the program's security policy. These actions can affect the data integrity, confidentiality, and availability of the application [111].

2.5.3 Countermeasures. It is necessary to verify the legitimacy of the applications and ensure sufficient control of the app stores to mitigate *spoofing attacks* [8]. In that regard, Landau et al. [79] proposed the use of applications developed by authorized organizations to ensure their trustworthiness. When it comes to *malware attacks*, the same countermeasures proposed for the *Data processing & conversion* phase also apply for applications. That is, the use of antivirus, firewall, Intrusion Detection Systems (IDS), and anomaly detection systems to identify and mitigate the attacks. Furthermore, Takabi et al. [164, 165] proposed the use of access control mechanisms over the information to restrict its access and thus mitigate confidentiality impacts. They also indicated the use of randomization and differential privacy. Besides, they proposed the integration of *homomorphic encryption* to operate with encrypted information combined with *functional encryption* to access only to a subset of the information.

As an opportunity for BCI, we identify some preventive actions against *misconfiguration attacks* defined by the Open Web Application Security Project (OWASP) [123], such as the use of minimal platforms with only necessary features, components, libraries, and software to reduce the probability of misconfiguration issues. Moreover, a periodic review and update of configuration parameters are also beneficial as part of the management process of applications. It is also necessary to create segmented application architectures that offer a division between components and defines different security groups, using Access Control Lists (ACLs).

Concerning *BO*, it is important to use programming languages that protect against these attacks, as well as the use of compilers with detection mechanisms. [147]. Developers must validate all inputs and follow well practice rules when using memory (e.g., verification of the boundaries of buffers). Moreover, sensitive applications must be ran using the lowest privileges possible and even isolated using sandbox techniques [110–112]. To detect *injection attacks*, both static and dynamic analysis of applications' source code have been proposed [134]. For their mitigation, it is necessary to escape all special characters included in the input [107, 134]. Multiple solutions have been proposed, such as the use of whitelists and blacklists [106], the use of safe languages and APIs containing automatic detection mechanisms [105, 134], the use of sandboxing techniques to define strict boundaries between processes [107], the definition of different permissions on the system [106], and error messages with minimal but descriptive details.

3 SECURITY ISSUES AFFECTING THE BCI DEPLOYMENTS

This section reviews the different architectural deployments of the BCI cycle found in the literature. After that, we group them into two main families, characterized by the BCI cycle implementation and its application scenario. In contrast to Section 2, where the security analysis

is independent of the deployment, this section reviews the state of the art of existing attacks affecting the devices implementing each phase of the BCI cycle, as well as their impacts and countermeasures. New opportunities, in terms of attacks and countermeasures, missed by the literature, are also highlighted in this section. Figure 4 represents both architectural deployments defined, Local BCIs, and Global BCIs, indicating the communication between their elements and the phases of the BCI cycle that each element implements according to the type of deployment.

3.1 Local BCI

3.1.1 Architecture Description. Local BCI deployments highlight by managing the neural data acquisition and stimulation processes of single users. This architecture typically deploys the BCI phases between two physical devices, as represented in Figure 4. The first one, identified as *BCI device*, focuses on the neural acquisition and stimulation procedures (phases 1 and 2 of the BCI cycle). In contrast, BCI applications (phase 5) run in a Near Control Device (NCD), a PC or smartphone that controls the BCI device using either a wired or wireless communication link. Phases 3 and 4 of the cycle can be implemented equally in both devices, where manufacturers make the final decision. At this point, it is essential to note that alternative designs can arise due to specific requirements of the deployments, such as the presence of multiple users. Moreover, we consider fully implantable BCIs within this architecture, since they require an external device for its configuration and verification.

3.1.2 Examples of Deployments. This kind of architectural deployment is the most commonly implemented for consumer-grade BCIs, where commercial brands like NeuroSky or Emotiv focus on scenarios such as gaming and entertainment [1, 96, 100]. Neuromedical scenarios also use this approach, where an Near Control Device (NCD) placed in the clinical environment manages the acquisition and stimulation processes. This section specifically addresses the issues detected in physical BCI devices, the inherent problems of the NCD, and those related to the communication between BCI and NCD. At this point, it is important to note that the attacks, impacts, and countermeasures detected for the BCI cycle are also applicable.

3.1.3 Attacks. Focusing on BCI devices, Ballarin et al. [8] identified attacks affecting the device *firmware* throw a configuration link (e.g., USB ports), having an impact on data integrity and confidentiality, also generating disruptions on the system. Pycroft et al. [136] identified the possibility of injecting malicious firmware updates. Moreover, we identify that these attacks can serve as an opportunity to generate safety problems. Ienca et al. [58, 59] documented *cryptographic attacks*, indicating that Cody's Emokit project was able to crack the encryption of data directly from the Emotiv EPOC, a consumer-grade BCI. They detected that these attacks affect data integrity and confidentiality. Marin et al. [95] detected that current Implantable Medical Devices (IMDs) lack robust security mechanisms. Yaqoob et al. [178] identified that neurostimulation devices lack encryption and usually define default passwords, impacting integrity and confidentially, easing unauthorized access to sensitive data. We also identify that they produce service availability and safety issues if they can modify the data.

The authors of References [24, 135] highlighted that attackers could focus on draining the battery of the device and thus affect both service availability and users' physical safety. In neurostimulation systems, losing the battery capacity would result in a loss of treatment, where the disease symptoms would reappear. Due to this, some IMDs include rechargeable batteries, reducing the risks of depleting them, and thus defining more robust solutions. It is also essential to consider that, in non-rechargeable systems, surgery is required to replace the batteries, increasing the risk of both physical and psychological safety issues.

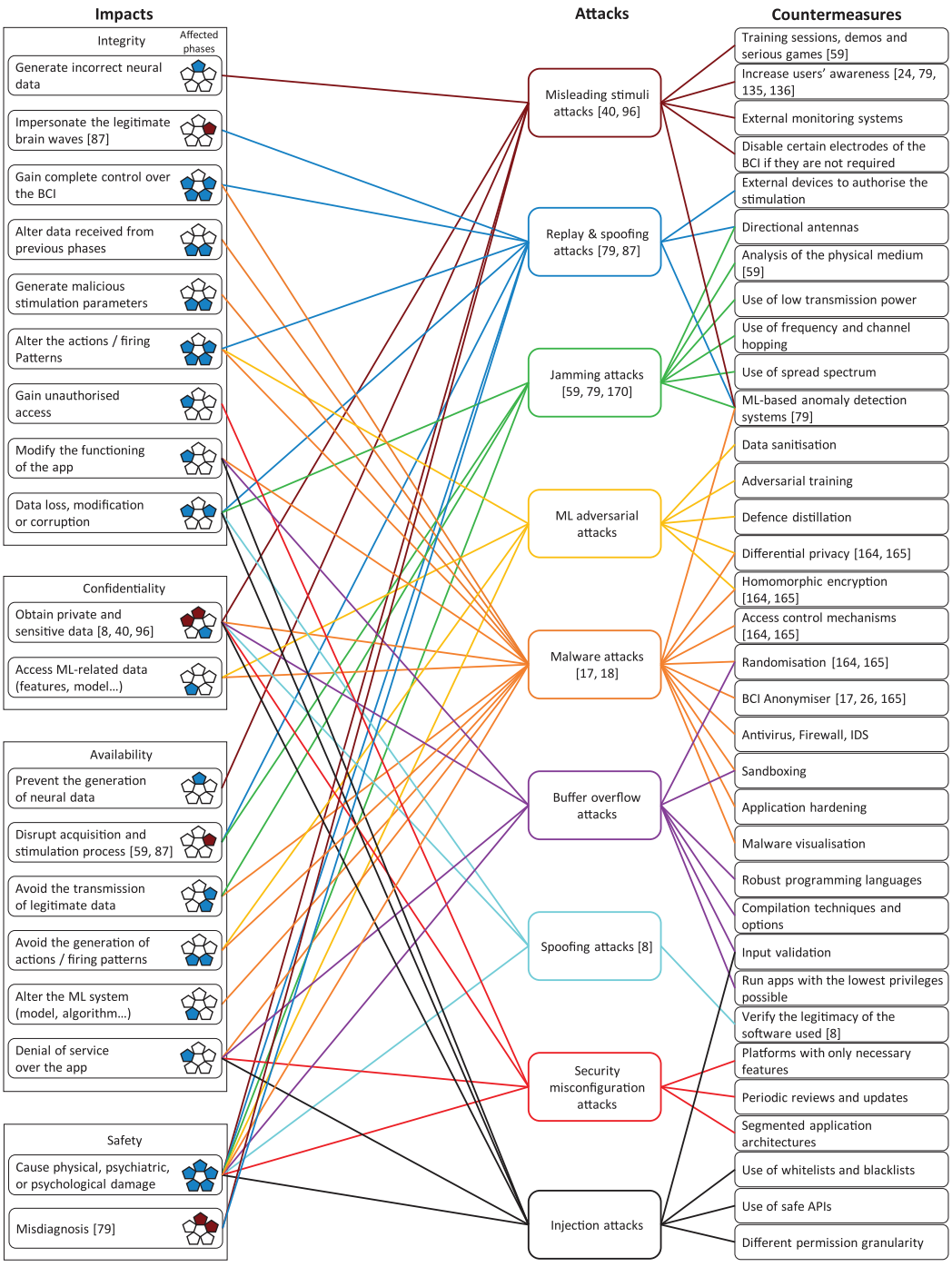

Fig. 3. Relationship between the attacks, impacts, and countermeasures over the BCI cycle. The phases of the cycle colored in red for each impact represent issues documented in the literature, while those marked in blue are our contribution. The attacks, impacts and countermeasures followed by references have been documented in the literature, and those without a cite represent our contribution.

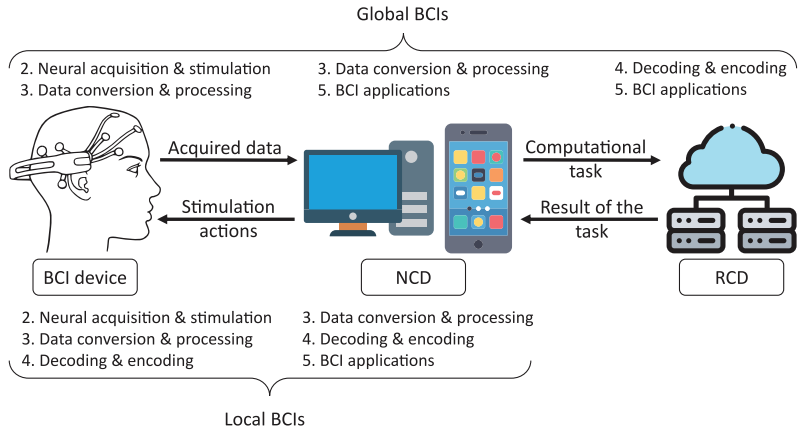

Fig. 4. Representation of Local BCI and Global BCI deployments, indicating the communication between their elements and the stages of the BCI cycle that each element implements according to the architectural deployment.

The authors of References [17, 136] described the possibility of *hijacking attacks*, referred to as *brainjacking*, where the attacker acquires complete access over the device by any means. These attacks generate an impact on all four security impact metrics. Finally, Pycroft et al. [135] identified general confidentiality impacts than can be shared by multiple attacks. They identified that close-loop IMDs use physiological data acquired by the BCI to improve the stimulation procedures or drug delivery. However, this sensitive data can be used by attackers to acquire information about the patient's health condition. Furthermore, an attacker can acquire sensitive information stored in the device, such as stimulation settings, personal data, or battery status, useful to perform new attacks.

Considering NCDs, Ballarin et al. [8] identified *social engineering and phishing attacks* against BCIs, focused on the acquisition of users' authentication credentials, affecting data confidentiality. Although BCI applications do not require a connection to the Internet, the NCD can be connected. Therefore, we detect that these systems can suffer *malware attacks* and, specifically, *ransomware* [2] and those based on *botnets* [74, 77, 159], with an impact on the integrity and availability of data and applications contained in the NCD, as well as users' safety. In particular, *botnets* also generate data confidentiality issues, since attackers have control over the system. Moreover, we detect *sniffing attacks* on NCDs taking advantage of networking configuration and protocols, such as MAC flooding, DHCP attacks, ARP spoofing, or DNS poisoning [5], affecting service and data integrity, confidentiality, and availability.

Focusing on the communication between BCI devices and NCDs, Sundararajan et al. [163] studied the security of the commercial-grade Emotiv Insight, which implemented Bluetooth Low Energy (BLE) in its version 4.0 to communicate with a smartphone that contains the application offered by Emotiv. They successfully performed *man-in-the-middle attacks* over the Bluetooth Low Energy (BLE) link, being able to intercept and modify information, force the BCI to perform unwanted tasks, and conduct *replay attacks* affecting, therefore, integrity, confidentiality, and availability of sensitive data. The literature has documented further integrity and confidentiality impacts, where attackers can intercept and modify sensitive data even using encryption [8, 79, 87, 95, 135, 163, 164]. These attacks are related to the *cryptographic attacks* described above, where weak encryption of the data stored in the device can derive in *man-in-the-middle attacks*. Finally,

it is important to note that the attacks related to user data and credentials have a higher impact if multiple users use the system.

3.1.4 Countermeasures. To some of the previous attacks, different countermeasures have been proposed. Related to *firmware attacks*, Ballarin et al. [8] indicated the encryption of the firmware, as well as an authenticity verification throw hash or signature. Pycroft et al. [136] highlighted periodic firmware updates and the use of authorization mechanisms for these updates. The authors of References [24, 135, 136] identified the use of access control mechanisms placed in external devices with proximity to the patient and anomaly detection systems over the BCI device usage to face potential threats such as *battery drain attacks*. In particular, for these attacks, rechargeable batteries are recommended to avoid a surgical replacement. The authors of Reference [79] proposed, as general countermeasures, the regulation of neurotechnology as a way to standardize its manufacturing processes, as well as a reduction of BCI training process, which tends to frustrate the users, being less willing to cooperate. These measures are complementary with those documented by Reference [135], which considered that BCI devices should keep logs and access events, including mechanisms for reporting bugs.

The use of robust cryptographic mechanisms and the latest protocol versions are determinant to avoid *cryptographic attacks*, *man-in-the-middle attacks*, and *sniffing attacks* [8, 163]. Besides, anonymization of the information transmitted from BCI to NCD is also recommendable against attacks impacting confidentiality, for example, using the BCI Anonymizer [17, 18, 164]. *Social engineering and phishing attacks* focused on credential theft can be reduced by implementing a second authentication factor to access the BCI and proper access control mechanisms [8, 135, 165]. The application of the *malware* countermeasures indicated in Section 2.3 can evade global *malware* threats impacting NCDs, by updating all software to the latest version and implementing periodic backup plans. Moreover, the use of ML techniques, as proposed by Fernández-Maimó et al. [37] for Medical Cyber-Physical Systems (MCPS), can also be used to detect, classify, and mitigate *ransomware attacks*. Concerning *botnets*, a wide variety of detection techniques have been detected by us for the BCI field, like the use of anomaly detection based on ML and signatures, the quarantine of infected devices, and the interruption of particular communication flows [4, 73, 92]. Finally, we consider that the recommendations of the U.S. Food and Drug Administration (FDA) for premarket and postmarket management of security in medical devices apply to BCI [150, 168, 169].

3.2 Global BCI

3.2.1 Architecture Description. Global BCI architectures focus on the management of neural data acquisition and neural stimulation of multiple users through an Internet connection. This architecture considers three devices to deploy the phases making up the BCI cycle, as can be seen in Figure 4. In this family, the BCI device remains focused on data acquisition and stimulation (phase 2), whereas the NCD is in charge of the execution of applications (phase 5), as well as conversion and processing actions (phase 3). Finally, the new element introduced in this architecture is the Remote Control Device (RCD), representing one or more external resources or services accessible via the Internet, such as cloud computing and storage. It typically implements phases 4 and 5 of the BCI cycle, as it has the resources to run more complex applications and information analysis. The main difference between this architecture and the one described for Local BCIs in Section 3.1 is that, in Local BCIs, the NCD does not send user information to external services (e.g., cloud). Finally, this section focuses on the problems associated with the communication between NCD and RCD, and the BCI-related attacks that can apply to RCDs. However, these later attacks are addressed in a general way, as specific cloud computing attacks are outside the scope of this article.

3.2.2 Examples of Deployments. This architectural deployment is the most innovative, as it allows the communication of multiples users with external services and the creation of complex deployments, where the data and information of every user are stored and managed in a shared infrastructure. From a commercial point of view, Emotiv allows users to contrast their data with the data stored by other users, as well as keep users' neural recordings in the cloud to visualize and manipulate them, also offering an API called Emotiv Cortex [35]. Besides, several companies worldwide provide distributed BCI services, as is the case of Lifelines Neuro [88], which offers a continuous EEG acquisition, storage, and visualization in their cloud platform. These scenarios are especially relevant in the context of personalized medicine and early diagnosis.

3.2.3 Attacks and Countermeasures. Considering the attacks on this deployment, the issues documented in Section 3.1 for Local BCIs are also applicable in this architecture. However, Global BCIs present higher risks, since these deployments are an opportunity for remote attacks against interconnected BCI devices, which derives in physical harm for their users. Furthermore, Takabi et al. [165] detected that BCI applications could send raw brain signals to cloud services that execute ML techniques to extract sensitive information and therefore affect confidentiality. We identify that this problem can also be present in Local BCIs if the NCD has an Internet connection. Ballarin et al. [8] identified that *man-in-the-middle attacks* could occur in the communication channel between NCD and RCD, affecting the integrity and confidentiality of the data transmitted as well as the service availability. They also detected that attacks on RCDs could have a higher impact on confidentiality than on Local BCIs, as these platforms store sensitive information from multiple users, that can be stolen or sold to third parties. Ienca et al. [60] detected different issues in Global BCIs in terms of their usage. First, they highlighted that current brands, such as Emotiv [34], indicate in their privacy policy that they can gather personal data, usage information, and interactions with other applications, and that they can infer information from these sources, with potential confidentiality issues. The authors identified as possible the use of big data to extract associations and share the data with third parties. Moreover, they detected that the use of cloud services could derive in a massive database theft with sensitive data, an unclear legal liability in case of breaches.

We identify that this architecture is quite similar to those defined and implemented for Internet of Things (IoT) scenarios, where constrained devices communicate with external services via intermediate systems, especially when multiple devices interact. We detect that most of the security attacks and impacts defined by Stellios et al. [160] are also applicable in this architecture. Moreover, we consider that the issues highlighted by the OWASP in their IoT projects are critical aspects of Global BCIs [125]. This relationship between IoT and external services has been previously studied in cloud computing scenarios [19]. Despite the advantages, attacks on cloud computing can impact integrity, confidentiality, and availability in different cloud architecture levels, such as infrastructure, networking, storage, and software [9, 155]. The evolution of NCDs derives in mobile devices with higher computing capabilities, integrated into mobile cloud computing systems. However, they also have an impact on the security of deployments [113]. We also detect that the improvement of NCDs capabilities can also allow the introduction of fog computing in Global BCIs, where NCDs perform part of the computation, generating new security and trust issues [93, 142, 183]. *Malware attacks* are also present in cloud environments, where ransomware and botnets are common threats [155].

Focusing on general cloud computing countermeasures, Amara et al. [3] identified security threats and attacks, as well as the mitigation techniques against them. The use of honeypots, firewalls, and IDS in cloud scenarios is convenient to reduce the impact of *malware attacks* [142].

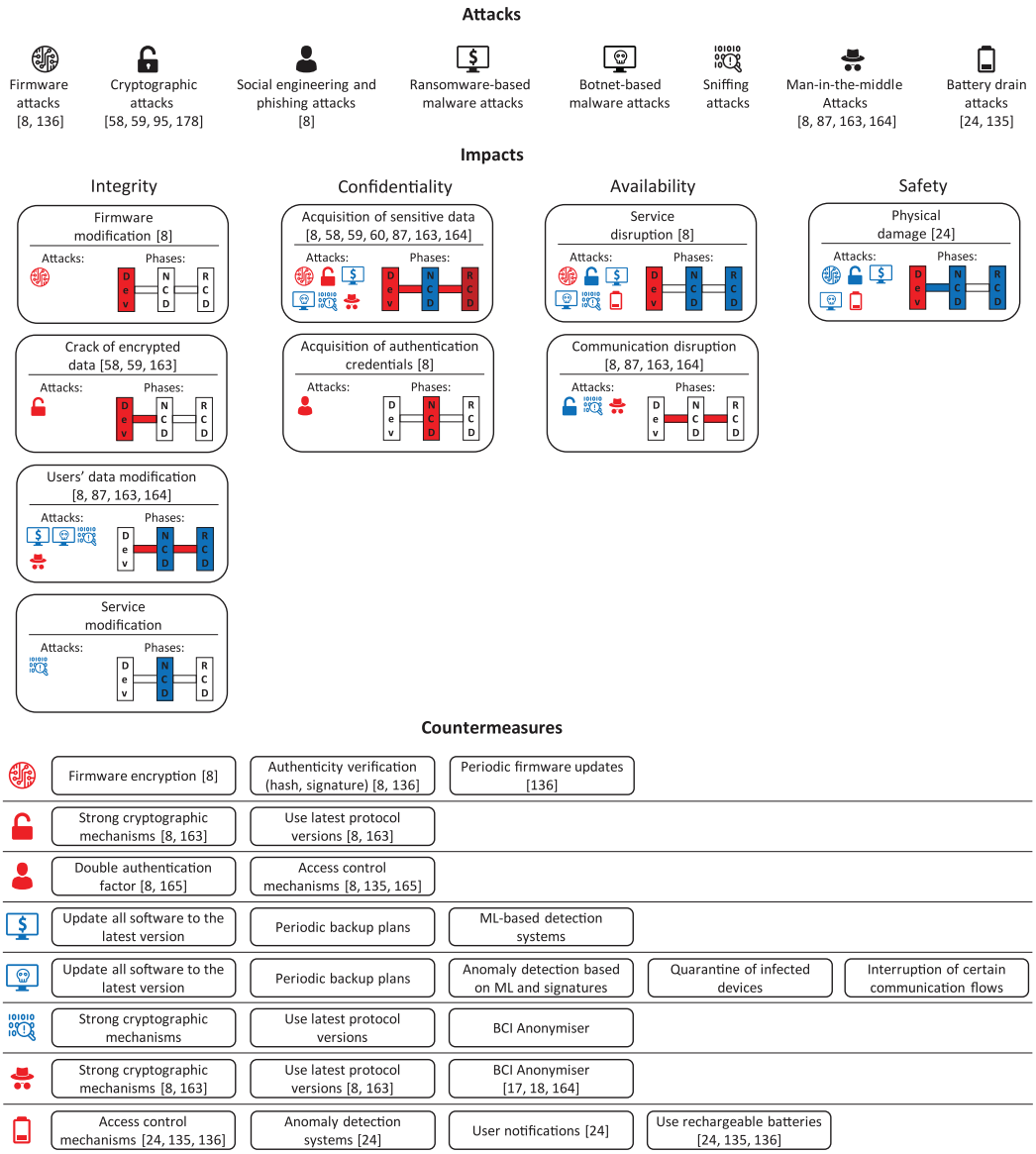

Fig. 5. Attacks, impacts, and countermeasures associated with the BCI architectural deployments. Elements indicated in red represent information detected in the literature, while blue represents our contribution.

Figure 5 summarizes the previous attacks, impacts, and countermeasures. This figure first shows the list of attacks considered in this section, associated with a unique icon, where those attacks with references indicate that they have been detected in the literature, while those without references represent our contribution. After that, we show the impacts that generate the previous attacks, organized by category. For each impact, we indicate the specific attacks that cause the impact, and which elements of the architectural deployments presented in Figure 4 are affected. Moreover, we consider the issues on the communication links between these elements. In particular, the attacks and elements identified in red represent issues detected in the literature, whereas those in blue are

our contributions. Finally, this figure lists countermeasures detected both in the literature and by us, associating each attack with a list of countermeasures. The color and reference criteria used before for the impacts also applies to the countermeasures, where an attack represented with a particular color indicates that all their countermeasures have the same color.

4 BCI TRENDS AND CHALLENGES

One of the first BCI solutions was developed at the end of the 1990s. It supposed a significant advancement in the medical industry, specifically in neurorehabilitation, bringing to the reality the mental control of prosthetic limbs and wheelchairs [119]. During the decade of the 2000s, a new generation of neuroprosthetic devices was developed to restore the mobility of patients severely paralyzed, creating communication links between the brain and a wide variety of actuators, such as robotic exoskeletons [82]. This trend in the field of BCI has resulted in new paradigms and scenarios in the last decade, where acquisition and stimulation procedures are used together to acquire brain activity and deliver feedback to the brain or peripheral nerves, defining the concept of bidirectional, or closed-loop, BCIs. Focusing on these systems, NeuroPace RNS is the only technology clinically approved for closed-loop treatment [33]. DBS is nowadays considered as a unidirectional BCI system, or open-loop, only performing stimulation actions. Nevertheless, current research aims to develop closed-loop DBS systems that are able to automatically identify the best stimulation parameters based on the status of the brain [52]. This evolution is also applicable for neuroprostheses, where the users can mentally control prosthesis while receiving stimulation to recover motor abilities [85].

This evolution allowed the definition of prospect ways of interaction where the BCI acts as an online communication element with other systems and users, based on Global BCI architectures. In particular, we subsequently present several examples of futuristic systems to highlight the importance of security in the progress of BCI technologies. Zhang et al. [182] defined the concept of the Internet of Brain, also known as Brain-to-Internet (BtI), where the BCI uses an NCD to access Internet services, such as search results or social media. Lebedev et al. [82] also described experiments where monkeys controlled remote robotic arms using BCI devices. More recently, Saad et al. [144] identified that 6G technologies could enable the interconnection of BCIs with the Internet. Besides, Martins et al. [97] documented a fusion between neuralnanorobotics and cloud services to acquire knowledge, defining the concept of Human Brain/Cloud Interface (B/CI). Another futuristic approach, Brain-to-Brain (BtB), allows direct communications between two brains, known as BtB [127, 184], where Pais-Vieira et al. [127] documented the real-time exchange of information between the brain of two rats. These systems have also been extended to create networks of interconnected brains, known as Brainet, which can perform collaborative tasks between users and share knowledge, memories, or thoughts through remote brains [67, 126]. Although these systems are in an early research stage, they could be a reality in the next decades, where security aspects will gain enormous importance. To represent this trend, Figure 6 illustrates this evolution of the literature, indicating the years of publication and approaches. Besides, current innovations, such as the use of silicon-based chips, could increase the quantity of information that we can acquire from the brain, and ease the development of electronic devices to improve the resolution of the neural acquisition and sensitivity of the process [121].

The BCI research field has gained relevance in the last few years, where different governments have funded and promoted BCI initiatives. In the United States of America, the DARPA is supporting the BRAIN Initiative (Brain Research through Advancing Innovative Neurotechnologies) [64]. Canada has launched its research line, called the Canadian Brain Research Strategy [63, 162]. On the other side of the Atlantic ocean, the European Union has also supported different projects, such as the Human Brain Project (HBP) [133] or the Brain/Neural Computer Interaction (BNCI)

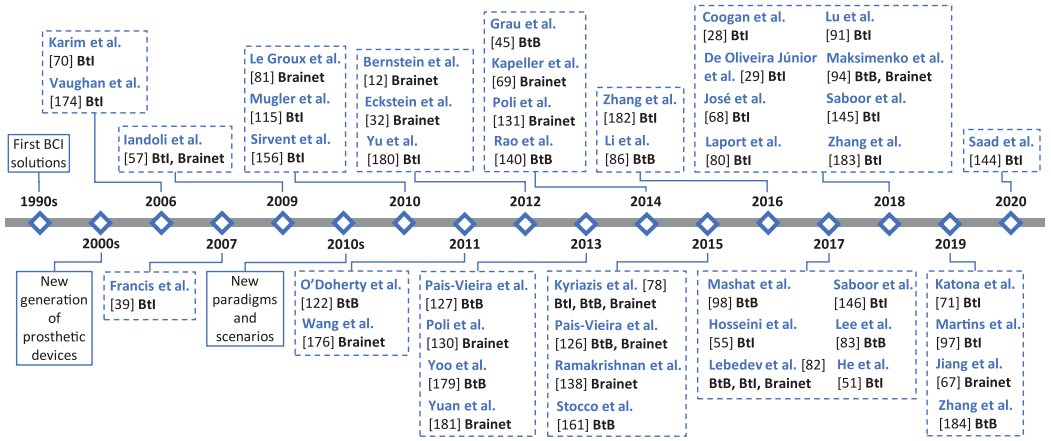

Fig. 6. Timeline of the evolution of BCI research, seen from the perspective of BtI, BtB, and Brainet approaches.

project [21, 22]. Asia has also promoted several initiatives, such as the China Brain Project [132] or the Brain/MINDS project in Japan [20]. All the previous initiatives and projects aim to advance the understanding of the human brain through the use of innovative technologies. As a consequence, emerging technologies offer precise acquisition and stimulation capabilities that enable new BCI application scenarios. The common interest in the study of the human brain and, in particular, on BCI leads to new opportunities for manufacturers, who can increase their competitiveness producing revolutionary BCI services based on growing paradigms such as the IoT, cloud computing, and big data. This development derives in the improvement of the usability, accuracy and safety of the products, together with their expansion to non-medical economic sectors such as entertainment. The result of the above is a trend of BCI toward Global BCI architecture deployments, where multiple BCI devices can communicate between them to perform collaborative tasks, based on the approaches of BtI, BtB, and Brainet. Once summarized the evolution of BCI and its trend, below, we highlight the most relevant current and future challenges concerning security on BCI.

4.1 Interoperability between BCI Deployments

Existing BCI deployments consider isolated devices without standards to provide interoperability in terms of communication and data representation. This is the case of commercial BCI brands and devices, which have been designed to resolve particular problems and are not compatible between them [137]. Moreover, deployments integrating the communication between several BCIs are ad hoc; that is, manufacturers design and implement them, considering only the requirements of a particular scenario. In this context, the current trend of BCIs toward paradigms such as the IoT and cloud computing will require an improvement in interoperability, as it is essential to ensure the future expansion of BCI technologies. Besides, the lack of interoperability limits the definition of global cybersecurity systems and mechanisms that can be applied. In this sense, current BCI solutions are device-oriented and do not offer collaborative mechanisms against cyberattacks. We detect as a future opportunity the use of well-known standardized APIs, communication technologies, and protocols to offer seamless protection on BCI. We also propose the use of ontologies to represent neural information in a formal and standardized fashion. Different companies and products would use a joint representation to ease data interpretation, processing, and sharing. This homogenization would have a positive impact on cybersecurity, enabling the

design and deployment of new protocols and mechanisms for the secure exchange of particular pieces of sensitive data between independent BCI solutions. In particular, the exchange of medical information between different organizations can be accomplished using well-known standards, as is the case of the HL7 standard [53].

4.2 Extensibility of BCI Designs

Extensibility refers to the ability of BCIs to add new functionality and application scenarios dynamically. Nowadays, BCI devices suffer a lack of extensibility, as companies manufacture them to provide particular services on fixed application scenarios. The neural data processing is performed in a fixed way and according to predefined premises. It means that each layer making up BCI architectures performs particular processing tasks, which can not be changed or even modified on demand [163]. Since each application scenario has its requirements and restrictions, the trend toward Global BCI will need new automatic and flexible architectures and processing mechanisms over the acquired neural data. These aspects also affect the security solutions that can be applied, since current constraints of BCI systems prevent the use of reactive and adaptive defensive mechanisms to face the threats described in previous sections. In conjunction with a lack of interoperability, the security responsibilities of each phase of the architecture are predefined and cannot be extended within that element, or delegated to be performed in other systems. As a future line of work, we highlight the design of BCI deployments that allow the implementation of most of the operations performed in software, instead of hardware, allowing developers to change the system's behavior. Another possible solution is a modular design of BCI, including supplementary modules, according to the requirements. However, these modifications introduce new security challenges, since software developments are more prone to errors and attacks, and new modular systems will address specific challenges, such as the verification of their authenticity.

4.3 Data Protection

Current BCI architectures and deployments do not consider the protection of neural data and personal information, as detected in the literature [137, 152, 164]. The evolution of BCIs toward distributed scenarios with heterogeneous and ubiquitous characteristics, such as BtB approaches, will require the storage and management of multiple users' personal and sensitive data. Because of that, future deployments should ensure that this critical information is transmitted and processed securely. Specifically, robust cryptography mechanisms need to be applied over data communication and storage, while techniques such as differential privacy or homomorphic encryption would help to ensure the anonymization of the data. Moreover, users do not have control over their privacy preferences to define who has access to the information and in which particular circumstances. Because of that, there are no specific privacy regulations to ensure that applications and external services can access only to the neural information accepted by users, nor any limitation on manufacturers or third-parties to prevent the processing of sensitive neural data without users authorization. To improve this situation, we propose policy-based solutions that allow users to define their privacy preferences based on their particular context. Besides, we propose the use of user-friendly systems that also help users proposing privacy-preserving recommendations. These initiatives must also align with the data protection law applicable in each country.

4.4 Physical and Architectural BCI Threats

Nowadays, a considerable amount of BCI designs and deployments do not consider cybersecurity issues such as the protection of communications, processing, storage, and applications. Although some solutions include security mechanisms, like Medtronic DBS products, some aspects must be improved. In particular, these devices use proprietary telemetry protocols [101], which recently

has led to vulnerabilities [27]. Nevertheless, companies such as Medtronic or Boston Scientific publish security bulletins when a security vulnerability affecting their devices is detected [103, 151], highlighting the interest that companies have on security. Moreover, the lack of BCI standards and, specifically, cybersecurity standards, prevent the homogenization of the security solutions implemented [17, 137, 163, 165]. The expansion of BCI will require robust dynamic cybersecurity mechanisms to face future challenges. Moreover, the development of more precise BCI devices and the integration of a large number of devices and systems, would result in a massive production of sensitive data. In our opinion, this context could benefit the increase of vulnerable systems and communication links. To address these challenges, manufacturers should evaluate alternatives for the mitigation of cyberattacks from multiple perspectives, aiming to implement seamless cybersecurity solutions. Based on that, we propose using 5G network technologies, since they have been designed to support a significant number of devices, which are necessary for BtB and Brainet scenarios. In particular, we identify that techniques and paradigms associated with 5G, such as Network Function Virtualisation (NFV) and Software-defined Networking (SDN) for the virtualization and dynamic management of network communications, are useful for the development of reactive cybersecurity solutions. Also, technologies such as Blockchain can provide the tracking of the information and ensure that it has not been modified, guaranteeing the integrity of the data. Moreover, we identify the protection of network communications by using protocols such as TLS [62] or IPsec [61] as an opportunity, which offers robust mechanisms against cyberattacks. Moreover, we detect that the application of information risk management standards, such as the ISO 27000 [65], and the NIST Cybersecurity Framework [120] could benefit the creation of homogeneous and robust solutions. Finally, we identify that game theory applied to BCI security strategies can be useful to implement regularly evolving systems. In particular, they can be useful to model how to establish the most appropriate countermeasures against continuously and automatically changing attacks, specifically in distributed scenarios such as BtB [7].

5 CONCLUSION

This article performs a global and comprehensive analysis of the literature of BCIs in terms of security and safety. Mainly, we have evaluated the attacks, impacts and countermeasures that BCI solutions suffer from the software's architectural design and implementation perspectives. Initially, we proposed a unified version of the BCI cycle to include neural data acquisition and stimulation processes. Once having a homogeneous BCI cycle design, we identified security attacks, impacts, and countermeasures affecting each phase of the cycle. It served as a starting point to determine which processes and functioning stages of BCIs are more prone to attacks. The architectural deployments of current BCI solutions have also been analyzed to highlight the security attacks and countermeasures related to each approach to understanding the issues of these technologies in terms of network communications. Finally, we provide our vision regarding BCI trends and depict that the current evolution of BCIs toward interconnected devices is generating tremendous security concerns and challenges, which will increase in the near future.

Among the learned lessons, we highlight the following five: (1) the field of security oriented to BCI technologies is not yet mature, generating opportunities for attackers; (2) even non-sophisticated attacks can have a significant impact on both BCI technologies and users' safety; (3) there is a current opportunity for standardization initiatives to unify BCIs in terms of information security; (4) well-studied fields, such as IMDs and IoT, can define a guide to develop robust security mechanisms for BCIs; (5) users' awareness of BCI security issues is vital.

As future work, we plan to focus our efforts on the design and implementation of solutions able to detect and mitigate attacks affecting the stimulation process in real time. In this context, we are considering using artificial intelligence techniques to detect anomalies in the firing patterns and

neural activity controlled by BCI solutions in charge of stimulating the brain. Besides, we also plan to contribute by improving the interoperability and data protection mechanisms of existing BCI architectures. Finally, another future work is the development of dynamic and proactive systems as an opportunity to mitigate the impacts of the attacks documented in this work.

ACKNOWLEDGMENT

We thank Mattia Zago for his advice during the development of the visual support of the work.

REFERENCES

[1] Minkyu Ahn, Mijin Lee, Jinyoung Choi, Sung Jun, Minkyu Ahn, Mijin Lee, Jinyoung Choi, and Sung Chan Jun. 2014. A review of brain-computer interface games and an opinion survey from researchers, developers and users. *Sensors* 14, 8 (Aug. 2014), 14601–14633.

[2] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* 74 (May 2018), 144–166.

[3] Naseer Amara, Huang Zhiqui, and Awais Ali. 2017. Cloud computing security threats and attacks with their mitigation techniques. In *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC'17)*. IEEE, 244–251.

[4] Pedram Amini, Muhammad Amin Araghizadeh, and Reza Azmi. 2015. A survey on Botnet: Classification, detection and defense. In *Proceedings of the International Electronics Symposium (IES'15)*. IEEE, 233–238.

[5] P. Anu and S. Vimala. 2017. A survey on sniffing attacks on computer networks. In *Proceedings of the International Conference on Intelligent Computing and Control (I2C2'17)*. IEEE, 5.

[6] P. Arico, G. Borghini, G. Di Flumeri, N. Sciaraffa, and F. Babiloni. 2018. Passive BCI beyond the lab: Current trends and future directions. *Physiol. Measure.* 39, 8 (Aug. 2018), 08TR02.

[7] A. Attiah, M. Chatterjee, and C. C. Zou. 2018. A game theoretic approach to model cyber attack and defense strategies. In *Proceedings of the IEEE International Conference on Communications (ICC'18)*. IEEE, 1–7.

[8] Pablo Ballarin Usieto and Javier Minguez. 2018. Avoiding brain hacking—Challenges of cybersecurity and privacy in Brain Computer Interfaces. Retrieved from https://www.bitbrain.com/blog/cybersecurity-brain-computer-interface.

[9] Srijita Basu, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, and Pritika Sarkar. 2018. Cloud computing security challenges & solutions-A survey. In *Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC'18)*. IEEE, 347–356.

[10] Nebia Bentabet and Nasr Eddine Berrached. 2016. Synchronous P300-based BCI to control home appliances. In *Proceedings of the 8th International Conference on Modelling, Identification and Control (ICMIC'16)*. IEEE, 835–838.

[11] S. López Bernal, A. Huertas Celdrán, L. Fernández Maimó, M. T. Barros, S. Balasubramaniam, and G. Martínez Pérez. 2020. Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. *IEEE Access* 8 (2020), 152204–152222.

[12] Abraham Bernstein, Mark Klein, and Thomas W. Malone. 2012. Programming the global brain. *Commun. ACM* 55, 5 (May 2012), 41.

[13] Meriem Bettayeb, Qassim Nasir, and Manar Abu Talib. 2019. Firmware update attacks and security for IoT devices. In *Proceedings of the ArabWIC 6th Annual International Conference Research Track*. ACM Press, 6.

[14] Marom Bikson, Andre R. Brunoni, Leigh E. Charvet, Vincent P. Clark, Leonardo G. Cohen, Zhi-De Deng, Jacek Dmochowski, Dylan J. Edwards, Flavio Frohlich, Emily S. Kappenman, Kelvin O. Lim, Colleen Loo, Antonio Mantovani, David P. McMullen, Lucas C. Parra, Michele Pearson, Jessica D. Richardson, Judith M. Rumsey, Pejman Sehatpour, David Sommers, Gozde Unal, Eric M. Wassermann, Adam J. Woods, and Sarah H. Lisanby. 2018. Rigor and reproducibility in research with transcranial electrical stimulation: An NIMH-sponsored workshop. *Brain Stimul.* 11, 3 (2018), 465–480.

[15] Gajanan K. Birajdar and Vijay H. Mankar. 2013. Digital image forgery detection using passive techniques: A survey. *Dig. Investigat.* 10, 3 (Oct. 2013), 226–245.

[16] Paul E. Black and Irena Bojanova. 2016. Defeating buffer overflow: A trivial but dangerous bug. *IT Profess.* 18, 6 (Nov 2016), 58–61.

[17] Tamara Bonaci, Ryan Calo, and Howard Jay Chizeck. 2015. App stores for the brain: Privacy and security in brain-computer interfaces. *IEEE Technol. Soc. Mag.* 34, 2 (June 2015), 32–39.

[18] Tamara Bonaci, Jeffrey Herron, Charles Matlack, and Howard Jay Chizeck. 2015. Securing the exocortex: A 21st-century cybernetics challenge. *IEEE Technol. Soc. Mag.* 34, 3 (Sep. 2015), 44–51. arxiv:hep-ph/0011146

[19] Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé. 2016. Integration of cloud computing and Internet of Things: A survey. *Future Gen. Comput. Syst.* 56 (Mar. 2016), 684–700.

[20] Brain/MINDS project. 2019. Brain/MINDS project. Retrieved from https://brainminds.jp/en/.
[21] Brain/Neural Computer Interaction project. 2015. Brain/Neural Computer Interaction project. Retrieved from http://bnci-horizon-2020.eu/.
[22] Clemens Brunner, Niels Birbaumer, Benjamin Blankertz, Christoph Guger, Andrea Kübler, Donatella Mattia, José del R. Millán, Felip Miralles, Anton Nijholt, Eloy Opisso, Nick Ramsey, Patric Salomon, and Gernot R. Müller-Putz. 2015. BNCI Horizon 2020: Towards a roadmap for the BCI community. *Brain-Comput. Interfaces* 2, 1 (Jan. 2015), 10.
[23] Carsten Buhmann, Torge Huckhagel, Katja Engel, Alessandro Gulberti, Ute Hidding, Monika Poetter-Nerger, Ines Goerendt, Peter Ludewig, Hanna Braass, Chi-un Choe, Kara Krajewski, Christian Oehlwein, Katrin Mittmann, Andreas K. Engel, Christian Gerloff, Manfred Westphal, Johannes A. Köppen, Christian K. E. Moll, and Wolfgang Hamel. 2017. Adverse events in deep brain stimulation: A retrospective long-term analysis of neurological, psychiatric and other occurrences. *PLoS ONE* 12, 7 (July 2017), 1–21.
[24] Carmen Camara, Pedro Peris-Lopez, and Juan E. Tapiador. 2015. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Info.* 55 (June 2015), 272–289.
[25] Debashis Das Chakladar and Sanjay Chakraborty. 2018. Feature extraction and classification in brain-computer interfacing: Future research issues and challenges. In *Natural Computing for Unsupervised Learning*. Springer, Cham, Chapter 5, 101–131.
[26] Howard Jay Chizeck and Tamara Bonaci. 2014. Brain-Computer Interface Anonymizer. U.S. Patent Application. US20140228701A1.
[27] Cybersecurity & Infrastructure Security Agancy (CISA). 2020. ICS Medical Advisory (ICSMA-19-080-01). Retrieved from https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01.
[28] Christopher G. Coogan and Bin He. 2018. Brain-computer interface control in a virtual reality environment and applications for the Internet of Things. *IEEE Access* 6 (2018), 10840–10849.
[29] Wilson G. de Oliveira Júnior, Juliana M. de Oliveira, Roberto Munoz, and Victor Hugo C. de Albuquerque. 2020. A proposal for Internet of Smart Home Things based on BCI system to aid patients with amyotrophic lateral sclerosis. *Neural Comput. Appl.* 32, 15 (Aug. 2020), 11007–11017.
[30] Till A. Dembek, Paul Reker, Veerle Visser-Vandewalle, Jochen Wirths, Harald Treuer, Martin Klehr, Jan Roediger, Haidar S. Dafsari, Michael T. Barbe, and Lars Timmermann. 2017. Directional DBS increases side-effect thresholds—A prospective, double-blind trial. *Move. Disord.* 32, 10 (2017), 1380–1388.
[31] Tamara Denning, Yoky Matsuoka, and Tadayoshi Kohno. 2009. Neurosecurity: Security and privacy for neural devices. *Neurosurg. Focus* 27, 1 (2009), E7.
[32] Miguel P. Eckstein, Koel Das, Binh T. Pham, Matthew F. Peterson, Craig K. Abbey, Jocelyn L. Sy, and Barry Giesbrecht. 2012. Neural decoding of collective wisdom with multi-brain computing. *NeuroImage* 59, 1 (Jan. 2012), 94–108.
[33] Christine A. Edwards, Abbas Kouzani, Kendall H. Lee, and Erika K. Ross. 2017. Neurostimulation devices for the treatment of neurologic disorders. *Mayo Clin. Proceed.* 92, 9 (2017), 1427–1444.
[34] Emotiv. 2019. Emotiv. Retrieved from https://www.emotiv.com/.
[35] Emotiv. 2019. Emotiv Cortex API. Retrieved from https://emotiv.github.io/cortex-docs/#introduction.
[36] Emotiv. 2019. EMOTIV EPOC+. Retrieved from https://www.emotiv.com/epoc/.
[37] Lorenzo Fernández Maimó, Alberto Huertas Celdrán, Ángel Perales Gómez, Félix García Clemente, James Weimer, and Insup Lee. 2019. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors* 19, 5 (Mar. 2019), 1114.
[38] Samuel G. Finlayson, John D. Bowers, Joichi Ito, Jonathan L. Zittrain, Andrew L. Beam, and Isaac S. Kohane. 2019. Adversarial attacks on medical machine learning. *Science* 363, 6433 (Mar. 2019), 1287–1289.
[39] Heylighen Francis. 2007. The global superorganism: An evolutionary-cybernetic model of the emerging network society. *Soc. Evol. Hist.* 6, 1 (2007), 58–119.
[40] Mario Frank, Tiffany Hwu, Sakshi Jain, Robert T. Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito, Ivo Sluganovic, and Dawn Song. 2017. Using EEG-based BCI devices to subliminally probe for private information. In *Proceedings of the on Workshop on Privacy in the Electronic Society (WPES'17)*. ACM Press, New York, New York, 133–136. Retrieved from https://arxiv:1312.6052.
[41] Jianwen Fu, Jingfeng Xue, Yong Wang, Zhenyan Liu, and Chun Shan. 2018. Malware visualization for fine-grained classification. *IEEE Access* 6 (2018), 14510–14523.
[42] Ariko Fukushima, Reiko Yagi, Norie Kawai, Manabu Honda, Emi Nishina, and Tsutomu Oohashi. 2014. Frequencies of inaudible high-frequency sounds differentially affect brain activity: Positive and negative hypersonic effects. *PLoS ONE* 9, 4 (Apr. 2014), e95464.
[43] Joyce Gomes-Osman, Aprinda Indahlastari, Peter J. Fried, Danylo L. F. Cabral, Jordyn Rice, Nicole R. Nissim, Serkan Aksu, Molly E. McLaren, and Adam J. Woods. 2018. Non-invasive brain stimulation: Probing intracortical circuits and improving cognition in the aging brain. *Front. Aging Neurosci.* 10 (2018), 177.

[44] Ian Goodfellow, Patrick McDaniel, and Nicolas Papernot. 2018. Making machine learning robust against adversarial inputs. *Commun. ACM* 61, 7 (July 2018), 56–66.
[45] Carles Grau, Romuald Ginhoux, Alejandro Riera, Thanh Lam Nguyen, Hubert Chauvat, Michel Berg, Julià L. Amengual, Alvaro Pascual-Leone, and Giulio Ruffini. 2014. Conscious brain-to-brain communication in humans using non-invasive technologies. *PLoS ONE* 9, 8 (Aug 2014), e105225.
[46] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197.
[47] Surbhi Gupta, Abhishek Singhal, and Akanksha Kapoor. 2017. A literature survey on social engineering attacks: Phishing attack. In *Proceedings of the IEEE International Conference on Computing, Communication and Automation (ICCCA'16)*. IEEE, 537–540.
[48] Christian J. Hartmann, Sabine Fliegen, Stefan J. Groiss, Lars Wojtecki, and Alfons Schnitzler. 2019. An update on best practice of deep brain stimulation in Parkinson's disease. *Therap. Adv. Neurol. Disord.* 12 (Jan. 2019), 1756286419838096.
[49] Joseph M. Hatfield. 2018. Social engineering in cybersecurity: The evolution of a concept. *Comput. Secur.* 73 (2018), 102–113.
[50] Vincent Haupert, Dominik Maier, Nicolas Schneider, Julian Kirsch, and Tilo Müller. 2018. Honey, I shrunk your app security: The state of android app hardening. In *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer International Publishing, Cham, 69–91.
[51] Shenghong He, Tianyou Yu, Zhenghui Gu, and Yuanqing Li. 2017. A hybrid BCI web browser based on EEG and EOG signals. In *Proceedings of the 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'17)*. IEEE, 1006–1009.
[52] Franz Hell, Carla Palleis, Jan H. Mehrkens, Thomas Koeglsperger, and Kai Bötzel. 2019. Deep brain stimulation programming 2.0: Future perspectives for target identification and adaptive closed loop stimulation. *Front. Neurol.* 10 (2019), 314.
[53] HL7 International. 2019. Health Level Seven. Retrieved from https://www.hl7.org/.
[54] Keum Shik Hong and Muhammad Jawad Khan. 2017. Hybrid brain-computer interface techniques for improved classification accuracy and increased number of commands: A review. *Front. Neurorobot.* 11 (July 2017), 35.
[55] Mohammad-Parsa Hosseini, Dario Pompili, Kost Elisevich, and Hamid Soltanian-Zadeh. 2017. Optimized deep learning for EEG big data and seizure prediction BCI via Internet of Things. *IEEE Trans. Big Data* 3, 4 (Dec. 2017), 392–404.
[56] Alberto Huertas Celdrán, Ginés Dólera Tormo, Félix Gómez Mármol, Manuel Gil Pérez, and Gregorio Martínez Pérez. 2016. Resolving privacy-preserving relationships over outsourced encrypted data storages. *Int. J. Info. Secur.* 15, 2 (Apr. 2016), 195–209.
[57] Luca Iandoli, Mark Klein, and Giuseppe Zollo. 2009. Enabling on-line deliberation and collective decision-making through large-scale argumentation. *Int. J. Decis. Supp. Syst. Technol.* 1, 1 (Jan. 2009), 69–92.
[58] Marcello Ienca. 2015. Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. *Bioethica Forum* 8, 2 (2015), 51–53.
[59] Marcello Ienca and Pim Haselager. 2016. Hacking the brain: Brain–computer interfacing technology and the ethics of neurosecurity. *Ethics Info. Technol.* 18, 2 (June 2016), 117–129.
[60] Marcello Ienca, Pim Haselager, and Ezekiel J. Emanuel. 2018. Brain leaks and consumer neurotechnology. *Nature Biotechnol.* 36, 9 (2018), 805–810.
[61] IETF. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Retrieved from https://tools.ietf.org/html/rfc6071.
[62] IETF. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. Retrieved from https://tools.ietf.org/html/rfc8446.
[63] Judy Illes, Samuel Weiss, Jaideep Bains, Jennifer A. Chandler, Patricia Conrod, Yves De Koninck, Lesley K. Fellows, Deanna Groetzinger, Eric Racine, Julie M. Robillard, and Marla B. Sokolowski. 2019. A neuroethics backbone for the evolving canadian brain research strategy.*Neuron* 101, 3 (Feb. 2019), 370–374.
[64] The BRAIN Initiative. 2019. The BRAIN Initiative. Retrieved from https://braininitiative.nih.gov/.
[65] ISO. 2018. ISO/IEC 27001 Information security management. Retrieved from https://www.iso.org/isoiec-27001-information-security.html.
[66] Matthew Jagielski, Alina Oprea, Battista Biggio, Chang Liu, Cristina Nita-Rotaru, and Bo Li. 2018. Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 19–35.
[67] Linxing Jiang, Andrea Stocco, Darby M. Losey, Justin A. Abernethy, Chantel S. Prat, and Rajesh P. N. Rao. 2019. BrainNet: A multi-person brain-to-brain interface for direct collaboration between brains. *Sci. Rep.* 9, 1 (Dec. 2019), 6115.

[68] Sergio José and Rodríguez Méndez. 2018. Modeling actuations in BCI-O. In *Proceedings of the 8th International Conference on the Internet of Things (IOT'18)*. ACM Press, New York, 6.
[69] Christoph Kapeller, Rupert Ortner, Gunther Krausz, Markus Bruckner, Brendan Z. Allison, Christoph Guger, and Günter Edlinger. 2014. Toward multi-brain communication: Collaborative spelling with a P300 BCI. In *Proceedings of the International Conference on Augmented Cognition*. Springer, Cham, 47–54.
[70] Ahmed A. Karim, Thilo Hinterberger, Jürgen Richter, Jürgen Mellinger, Nicola Neumann, Herta Flor, Andrea Kübler, and Niels Birbaumer. 2006. Neural Internet: Web surfing with brain potentials for the completely paralyzed. *Neurorehab. Neural Repair* 20, 4 (Dec. 2006), 508–515.
[71] Jozsef Katona, Tibor Ujbanyi, Gergely Sziladi, and Attila Kovari. 2019. *Electroencephalogram-based Brain-Computer Interface for Internet of Robotic Things*. Springer International Publishing, Cham, Chapter 12, 253–275.
[72] Elena Khabarova, Natalia Denisova, Aleksandr Dmitriev, Konstantin Slavin, and Leo Verhagen Metman. 2018. Deep brain stimulation of the subthalamic nucleus in patients with parkinson disease with prior pallidotomy or thalamotomy. *Brain Sci.* 8, 4 (Apr. 2018), 66.
[73] G. Kirubavathi and R. Anitha. 2018. Structural analysis and detection of android botnets using machine learning techniques. *Int. J. Info. Secur.* 17, 2 (Apr. 2018), 153–167.
[74] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.
[75] Jan Kubanek. 2018. Neuromodulation with transcranial focused ultrasound.*Neurosurg. Focus* 44, 2 (Feb. 2018), E14.
[76] D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang. 2001. *Introduction to Public Key Technology and the Federal PKI Infrastructure*. Technical Report. National Institute of Standards and Technology, 1–54. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.
[77] James Kurose and Keith Ross. 2017. *Computer Networking: A Top-Down Approach* (7th ed.). Pearson, London, 852 pages.
[78] Marios Kyriazis. 2015. Systems neuroscience in focus: From the human brain to the global brain? *Front. Syst. Neurosci.* 9 (Feb. 2015), 7.
[79] Ofir Landau, Rami Puzis, and Nir Nissim. 2020. Mind your mind. *Comput. Surveys* 53, 1 (2020), 1–38.
[80] Francisco Laport, Francisco J. Vazquez-Araujo, Paula M. Castro, Adriana Dapena, Francisco Laport, Francisco J. Vazquez-Araujo, Paula M. Castro, and Adriana Dapena. 2018. Brain-computer interfaces for Internet of Things. *Proceedings* 2, 18 (Sep. 2018), 1179.
[81] Sylvain Le Groux, Jonatas Manzolli, Paul F. Verschure, Marti Sanchez, Andre Luvizotto, Anna Mura, Aleksander Valjamae, Christoph Guger, Robert Prueckl, and Ulysses Bernardet. 2010. Disembodied and collaborative musical interaction in the multimodal brain orchestra. In *Proceedings of the International Conference on New Interfaces for Musical Expression*. MIME, 309–314.
[82] Mikhail A. Lebedev and Miguel A. L. Nicolelis. 2017. Brain-machine interfaces: From basic science to neuroprostheses and neurorehabilitation. *Physiol. Rev.* 97, 2 (Apr. 2017), 767–837.
[83] Wonhye Lee, Suji Kim, Byeongnam Kim, Chungki Lee, Yong An Chung, Laehyun Kim, and Seung-Schik Yoo. 2017. Non-invasive transmission of sensorimotor information in humans using an EEG/focused ultrasound brain-to-brain interface. *PLoS ONE* 12, 6 (July 2017), e0178476.
[84] M. León Ruiz, M. L. Rodríguez Sarasa, L. Sanjuán Rodríguez, J. Benito-León, E. García-Albea Ristol, and S. Arce Arce. 2018. Current evidence on transcranial magnetic stimulation and its potential usefulness in post-stroke neurorehabilitation: Opening new doors to the treatment of cerebrovascular disease. *Neurología (English Edition)* 33, 7 (2018), 459–472.
[85] Timothée Levi, Paolo Bonifazi, Paolo Massobrio, and Michela Chiappalone. 2018. Editorial: Closed-loop systems for next-generation neuroprostheses. *Front. Neurosci.* 12 (2018), 26.
[86] Guangye Li and Dingguo Zhang. 2016. Brain-computer interface controlled cyborg: Establishing a functional information transfer pathway from human brain to cockroach brain. *PLoS ONE* 11, 3 (Mar. 2016), e0150667.
[87] Qianqian Li, Ding Ding, and Mauro Conti. 2015. Brain-computer interface applications: Security and privacy challenges. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS'15)*. IEEE, 663–666.
[88] Lifelines Neuro. 2020. Neurodiagnostics Without Boundaries. Retrieved from https://www.lifelinesneuro.com/.
[89] Anli Liu, Mihály Vöröslakos, Greg Kronberg, Simon Henin, Matthew R. Krause, Yu Huang, Alexander Opitz, Ashesh Mehta, Christopher C. Pack, Bart Krekelberg, Antal Berényi, Lucas C. Parra, Lucia Melloni, Orrin Devinsky, and György Buzsáki. 2018. Immediate neurophysiological effects of transcranial electrical stimulation. *Nature Commun.* 9, 1 (Nov. 2018), 5092.
[90] Qiang Liu, Pan Li, Wentao Zhao, Wei Cai, Shui Yu, and Victor C. M. Leung. 2018. A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access* 6 (2018), 12103–12117.
[91] Huimin Lu, Hyoungseop Kim, Yujie Li, and Yin Zhang. 2018. BrainNets: Human emotion recognition using an Internet of Brian Things platform. In *Proceedings of the 14th International Wireless Communications and Mobile Computing Conference (IWCMC'18)*. IEEE, 1313–1316.

[92] Muhammad Mahmoud, Manjinder Nir, and Ashraf Matrawy. 2015. A survey on botnet architectures, detection and defences. *Int. J. Netw. Secur.* 17, 3 (May 2015), 272–289.

[93] Redowan Mahmud, Ramamohanarao Kotagiri, and Rajkumar Buyya. 2018. Fog computing: A taxonomy, survey and future directions. In *Internet of Everything*. Springer, Singapore, 103–130.

[94] Vladimir A. Maksimenko, Alexander E. Hramov, Nikita S. Frolov, Annika Lüttjohann, Vladimir O. Nedaivozov, Vadim V. Grubov, Anastasia E. Runnova, Vladimir V. Makarov, Jürgen Kurths, and Alexander N. Pisarchik. 2018. Increasing human performance by sharing cognitive load using brain-to-brain interface. *Front. Neurosci.* 12 (Dec. 2018), 949.

[95] Eduard Marin, Dave Singelée, Bohan Yang, Vladimir Volski, Guy A. E. Vandenbosch, Bart Nuttin, and Bart Preneel. 2018. Securing wireless neurostimulators. In *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY'18)*. Association for Computing Machinery, New York, NY, 287–298.

[96] Ivan Martinovic, Doug Davies, and Mario Frank. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the 21st USENIX Security Symposium*. USENIX, Bellevue, WA, 143–158.

[97] Nuno R. B. Martins, Amara Angelica, Krishnan Chakravarthy, Yuriy Svidinenko, Frank J. Boehm, Ioan Opris, Mikhail A. Lebedev, Melanie Swan, Steven A. Garan, Jeffrey V. Rosenfeld, Tad Hogg, and Robert A. Freitas. 2019. Human brain/cloud interface. *Front. Neurosci.* 13 (Mar. 2019), 112.

[98] M. Ebrahim M. Mashat, Guangye Li, and Dingguo Zhang. 2017. Human-to-human closed-loop control based on brain-to-brain interface and muscle-to-muscle interface. *Sci. Rep.* 7, 1 (Dec. 2017), 11001.

[99] Hideyuki Matsumoto and Yoshikazu Ugawa. 2017. Adverse events of tDCS and tACS: A review. *Clin. Neurophysiol. Pract.* 2 (2017), 19–25.

[100] M. McMahon and M. Schukat. 2018. A low-cost, open-source, BCI- VR game control development environment prototype for game-based neurorehabilitation. In *Proceedings of the IEEE Games, Entertainment, Media Conference (GEM'18)*. IEEE, 1–9.

[101] Medtronic. 2020. DBS Security Reference Guide. Retrieved from http://manuals.medtronic.com/content/dam/emanuals/neuro/NDHF1550-189563.pdf.

[102] Medtronic. 2020. DBS Theraphy for OCD. Retrieved from https://www.medtronic.com/us-en/patients/treatments-therapies/deep-brain-stimulation-ocd/about/risks-probable-benefits.html.

[103] Medtronic. 2020. Security Bulletins. Retrieved from https://global.medtronic.com/xg-en/product-security/security-bulletins.html.

[104] Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis, and Michalis Polychronakis. 2017. Spotless sandboxes: Evading malware analysis systems using wear-and-tear artifacts. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'17)*. IEEE, 1009–1024.

[105] MITRE. 2019. CWE-CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ("Injection") (3.2). Retrieved from https://cwe.mitre.org/data/definitions/74.html.

[106] MITRE. 2019. CWE-CWE-77: Improper Neutralization of Special Elements used in a Command ("Command Injection") (3.2). Retrieved from https://cwe.mitre.org/data/definitions/77.html.

[107] MITRE. 2019. CWE-CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection") (3.2). Retrieved from https://cwe.mitre.org/data/definitions/78.html.

[108] MITRE. 2019. CWE-CWE-89: Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection") (3.2). Retrieved from https://cwe.mitre.org/data/definitions/89.html.

[109] MITRE. 2019. CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer. Retrieved from https://cwe.mitre.org/data/definitions/119.html.

[110] MITRE. 2019. CWE-120: Buffer Copy without Checking Size of Input ("Classic Buffer Overflow") (3.2). Retrieved from https://cwe.mitre.org/data/definitions/120.html.

[111] MITRE. 2019. CWE-121: Stack-based Buffer Overflow (3.2). Retrieved from https://cwe.mitre.org/data/definitions/121.html.

[112] MITRE. 2019. CWE-122: Heap-based Buffer Overflow (3.2). Retrieved from https://cwe.mitre.org/data/definitions/122.html.

[113] Muhammad Baqer Mollah, Md. Abul Kalam Azad, and Athanasios Vasilakos. 2017. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *J. Netw. Comput. Appl.* 84 (Apr. 2017), 38–54.

[114] Ingrid Moreno-Duarte, Nigel Gebodh, Pedro Schestatsky, Berkan Guleyupoglu, Davide Reato, Marom Bikson, and Felipe Fregni. 2014. Chapter 2—Transcranial electrical stimulation: Transcranial Direct Current Stimulation (tDCS), Transcranial Alternating Current Stimulation (tACS), Transcranial Pulsed Current Stimulation (tPCS), and Transcranial Random Noise Stimulation (tRNS). In *The Stimulated Brain*, Roi Cohen Kadosh (Ed.). Academic Press, San Diego, 35–59.

[115] Emily M. Mugler, Carolin A. Ruf, Sebastian Halder, Michael Bensch, and Andrea Kubler. 2010. Design and implementation of a P300-based brain-computer interface for controlling an Internet browser. *IEEE Trans. Neural Syst. Rehab. Eng.* 18, 6 (Dec. 2010), 599–609.

[116] Elon Musk and Neuralink. 2019. An integrated brain-machine interface platform with thousands of channels. *bioRxiv* (2019). Retrieved from arXiv:https://www.biorxiv.org/content/early/2019/08/02/703801.full.pdf.

[117] NeuroPace. 2013. NeuroPace® RNS® System Patient Manual. Retrieved from https://www.accessdata.fda.gov/cdrh_docs/pdf10/p100026c.pdf.

[118] NeuroSky. 2019. NeuroSky. Retrieved from http://neurosky.com/.

[119] Miguel A. L. Nicolelis. 2001. Actions from thoughts. *Nature* 409, 6818 (2001), 403–407.

[120] NIST. 2018. Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework.

[121] Abdulmalik Obaid, Mina-Elraheb Hanna, Yu-Wei Wu, Mihaly Kollo, Romeo Racz, Matthew R. Angle, Jan Müller, Nora Brackbill, William Wray, Felix Franke, E. J. Chichilnisky, Andreas Hierlemann, Jun B. Ding, Andreas T. Schaefer, and Nicholas A. Melosh. 2020. Massively parallel microwire arrays integrated with CMOS chips for neural recording. *Sci. Adv.* 6, 12 (2020). Retrieved from arXiv:https://advances.sciencemag.org/content/6/12/eaay2789.full.pdf.

[122] Joseph E. O'Doherty, Mikhail A. Lebedev, Peter J. Ifft, Katie Z. Zhuang, Solaiman Shokur, Hannes Bleuler, and Miguel A. L. Nicolelis. 2011. Active tactile exploration using a brain–machine–brain interface. *Nature* 479, 7372 (Nov. 2011), 228–231.

[123] Open Web Application Security Project. 2017. Top 10-2017 A6-Security Misconfiguration-OWASP. Retrieved from https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration.

[124] Open Web Application Security Project. 2017. Top 10-2017 Top 10-OWASP. Retrieved from https://www.owasp.org/index.php/Top_10-2017_Top_10.

[125] Open Web Application Security Project. 2018. OWASP Internet of Things Project. Retrieved from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

[126] Miguel Pais-Vieira, Gabriela Chiuffa, Mikhail Lebedev, Amol Yadav, and Miguel A. L. Nicolelis. 2015. Building an organic computing device with multiple interconnected brains. *Sci. Rep.* 5, 1 (Dec. 2015), 11869.

[127] Miguel Pais-Vieira, Mikhail Lebedev, Carolina Kunicki, Jing Wang, and Miguel A. L. Nicolelis. 2013. A brain-to-brain interface for real-time sharing of sensorimotor information. *Sci. Rep.* 3, 1 (Dec. 2013), 1319.

[128] Mahboubeh Parastarfeizabadi and Abbas Z. Kouzani. 2017. Advances in closed-loop deep brain stimulation devices. *J. NeuroEngineer. Rehab.* 14, 1 (Aug. 2017), 79.

[129] Rafael Polanía, Michael A. Nitsche, and Christian C. Ruff. 2018. Studying and modifying brain function with non-invasive brain stimulation. *Nature Neurosci.* 21, 2 (Feb. 2018), 174–187.

[130] Riccardo Poli, Caterina Cinel, Ana Matran-Fernandez, Francisco Sepulveda, and Adrian Stoica. 2013. Towards cooperative brain-computer interfaces for space navigation. In *Proceedings of the International Conference on Intelligent User Interfaces (IUI'13)*. ACM Press, New York, 149.

[131] Riccardo Poli, Davide Valeriani, and Caterina Cinel. 2014. Collaborative brain-computer interface for aiding decision-making. *PLoS ONE* 9, 7 (July 2014), 22.

[132] Mu-ming Poo, Jiu-lin Du, Nancy Y. Ip, Zhi-Qi Xiong, Bo Xu, and Tieniu Tan. 2016. China brain project: Basic neuroscience, brain diseases, and brain-inspired computing. *Neuron* 92, 3 (Nov. 2016), 591–596.

[133] Human Brain Project. 2019. Human Brain Project. Retrieved from https://www.humanbrainproject.eu/en/.

[134] Open Web Application Security Project. 2017. Top 10-2017 A1-Injection-OWASP. Retrieved from https://www.owasp.org/index.php/Top_10-2017_A1-Injection.

[135] Laurie Pycroft and Tipu Z. Aziz. 2018. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Rev. Med. Devices* 15, 6 (July 2018), 403–406.

[136] Laurie Pycroft, Sandra G. Boccard, Sarah L.F. Owen, John F. Stein, James J. Fitzgerald, Alexander L. Green, and Tipu Z. Aziz. 2016. Brainjacking: Implant security issues in invasive neuromodulation. *World Neurosurg.* 92 (Aug. 2016), 454–462.

[137] Rabie A. Ramadan and Athanasios V. Vasilakos. 2017. Brain computer interface: Control signals review. *Neurocomput.* 223 (Feb. 2017), 26–44.

[138] Arjun Ramakrishnan, Peter J. Ifft, Miguel Pais-Vieira, Yoon Woo Byun, Katie Z. Zhuang, Mikhail A. Lebedev, and Miguel A.L. Nicolelis. 2015. Computing arm movements with a monkey Brainet. *Sci. Rep.* 5, 1 (Sep. 2015), 10767.

[139] Rajesh P. N. Rao. 2019. Towards neural co-processors for the brain: Combining decoding and encoding in brain–computer interfaces. *Curr. Opin. Neurobiol.* 55 (Apr. 2019), 142–151.

[140] Rajesh P. N. Rao, Andrea Stocco, Matthew Bryan, Devapratim Sarma, Tiffany M. Youngquist, Joseph Wu, and Chantel S. Prat. 2014. A direct brain-to-brain interface in humans. *PLoS ONE* 9, 11 (Nov. 2014), e111332.

[141] Heena Rathore, Chenglong Fu, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani, and Zhengtao Yu. 2020. Multi-layer security scheme for implantable medical devices. *Neural Comput. Appl.* 32, 9 (2020), 4347–4360.

[142] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. 2018. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gen. Comput. Syst.* 78 (Jan. 2018), 680–698.

[143] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. 2019. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. Technical Report. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

[144] W. Saad, M. Bennis, and M. Chen. 2019. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Netw.* (2019), 1–9.

[145] Abdul Saboor, Felix Gembler, Mihaly Benda, Piotr Stawicki, Aya Rezeika, Roland Grichnik, and Ivan Volosyak. 2018. A browser-driven SSVEP-based BCI web speller. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC'18)*. IEEE, Miyazaki, Japan, 625–630.

[146] Abdul Saboor, Aya Rezeika, Piotr Stawicki, Felix Gembler, Mihaly Benda, Thomas Grunenberg, and Ivan Volosyak. 2017. SSVEP-based BCI in a smart home scenario. In *Proceedings of the International Work-Conference on Artificial Neural Networks*. Springer, Cham, 474–485.

[147] Takamichi Saito, Ryohei Watanabe, Shuta Kondo, Shota Sugawara, and Masahiro Yokoyama. 2016. A survey of prevention/mitigation against memory corruption attacks. In *Proceedings of the 19th International Conference on Network-based Information Systems (NBiS'16)*. IEEE, 500–505.

[148] Parthana Sarma, Prakash Tripathi, Manash Pratim Sarma, and Kandarpa Kumar Sarma. 2016. Pre-processing and feature extraction techniques for EEG-BCI applications—A review of recent research. *ADBU-J. Eng. Technol.* 5 (2016), 2348–7305.

[149] M. A. Scholl, K. M. Stine, J. Hash, P. Bowen, L. A. Johnson, C. D. Smith, and D. I. Steinberg. 2008. *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

[150] Suzanne B. Schwartz. 2018. Medical device cybersecurity through the FDA lens. In *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, Baltimore, MD.

[151] Boston Scientific. 2020. Product Security Information. Retrieved from https://www.bostonscientific.com/en-US/customer-service/product-security/product-security-information.html.

[152] Diego Sempreboni and Luca Viganò. 2018. Privacy, Security, and Trust in the Internet of Neurons. Retrieved from https://arxiv:cs.CY/1807.06077.

[153] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. 2017. Membership inference attacks against machine learning models. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 3–18.

[154] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi. 2019. A Survey on malware analysis and mitigation techniques. *Comput. Sci. Rev.* 32 (May 2019), 23.

[155] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. 2016. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* 75 (Nov. 2016), 200–222.

[156] José L. Sirvent, José M. Azorín, Eduardo Iáñez, Andrés Úbeda, and Eduardo Fernández. 2010. P300-based brain-computer interface for Internet browsing. In *Trends in Practical Applications of Agents and Multiagent Systems*. Springer, Berlin, 615–622.

[157] International Neuromodulation Society. 2020. International Neuromodulation Society. Retrieved from https://www.neuromodulation.com/.

[158] Kandhasamy Sowndhararajan, Minju Kim, Ponnuvel Deepa, Se Park, and Songmun Kim. 2018. Application of the P300 event-related potential in the diagnosis of epilepsy disorder: A review. *Scientia Pharmaceutica* 86, 2 (Mar. 2018), 10.

[159] William Stallings. 2017. *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson, London, 766 pages.

[160] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. 2018. A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surveys Tutor.* 20, 4 (2018), 3453–3495.

[161] Andrea Stocco, Chantel S. Prat, Darby M. Losey, Jeneva A. Cronin, Joseph Wu, Justin A. Abernethy, and Rajesh P. N. Rao. 2015. Playing 20 questions with the mind: Collaborative problem solving by humans using a brain-to-brain interface. *PLoS ONE* 10, 9 (Sep 2015), e0137303.

[162] Canadian Brain Research Strategy. 2019. Canadian Brain Research Strategy. Retrieved from https://canadianbrain.ca/.

[163] Kaushik Sundararajan. 2017. *Privacy and Security Issues in Brain Computer Interface*. Master's thesis. Auckland University of Technology.

[164] Hassan Takabi. 2016. Firewall for brain: Towards a privacy preserving ecosystem for BCI applications. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS'16)*. IEEE, 370–371.

[165] Hassan Takabi, Anuj Bhalotiya, and Manar Alohaly. 2016. Brain computer interface (BCI) applications: Privacy threats and countermeasures. In *Proceedings of the IEEE 2nd International Conference on Collaboration and Internet Computing*. IEEE, 102–111.

[166] Andrew S. Tanenbaum and David J. Wetherall. 2011. *Computer Networks* (5th ed.). Pearson, London.
[167] William J. Tyler, Joseph L. Sanguinetti, Maria Fini, and Nicholas Hool. 2017. Non-invasive neural stimulation. In *Micro- and Nanotechnology Sensors, Systems, and Applications IX*, Thomas George, Achyut K. Dutta, and M. Saif Islam (Eds.), Vol. 10194. International Society for Optics and Photonics, Anaheim, CA, 280–290.
[168] U.S. Food and Drug Administration. 2016. *Postmarket Management of Cybersecurity in Medical Devices*. Technical Report. U.S. Food and Drug Administration, Rockville, MD.
[169] U.S. Food and Drug Administration. 2018. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Technical Report. U.S. Food and Drug Administration, Rockville, MD.
[170] Satish Vadlamani, Burak Eksioglu, Hugh Medal, and Apurba Nandi. 2016. Jamming attacks on wireless networks: A taxonomic survey. *Int. J. Prod. Econ.* 172 (Feb. 2016), 76–94.
[171] Swati Vaid, Preeti Singh, and Chamandeep Kaur. 2015. EEG signal analysis for BCI interface: A review. In *Proceedings of the International Conference on Advanced Computing and Communication Technologies (ACCT'15)*. IEEE, 143–147.
[172] Marcel van Gerven, Jason Farquhar, Rebecca Schaefer, Rutger Vlek, Jeroen Geuze, Anton Nijholt, Nick Ramsey, Pim Haselager, Louis Vuurpijl, Stan Gielen, and Peter Desain. 2009. The brain–computer interface cycle. *J. Neural Eng.* 6, 4 (Aug. 2009), 041001.
[173] Sebastian Vasile, David Oswald, and Tom Chothia. 2019. Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices. In *Smart Card Research and Advanced Applications*. Springer, Cham, 171–185.
[174] T. M. Vaughan, D. J. Mcfarland, G. Schalk, W. A. Sarnacki, D. J. Krusienski, E. W. Sellers, and J. R. Wolpaw. 2006. The wadsworth BCI research and development program: At home with BCI. *IEEE Trans. Neural Syst. Rehab. Eng.* 14, 2 (June 2006), 229–233.
[175] Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak, and Muhammad Rezal Kamel Ariffin. 2014. Passive video forgery detection techniques: A survey. In *Proceedings of the 10th International Conference on Information Assurance and Security*. IEEE, 29–34.
[176] Yijun Wang and Tzyy-Ping Jung. 2011. A collaborative brain-computer interface for improving human performance. *PLoS ONE* 6, 5 (May 2011), e20422.
[177] Ping Yan and Zheng Yan. 2018. A survey on dynamic mobile malware detection. *Softw. Qual. J.* 26, 3 (Sep. 2018), 891–919.
[178] T. Yaqoob, H. Abbas, and M. Atiquzzaman. 2019. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Commun. Surveys Tutor.* 21, 4 (2019), 3723–3768.
[179] Seung-Schik Yoo, Hyungmin Kim, Emmanuel Filandrianos, Seyed Javid Taghados, and Shinsuk Park. 2013. Non-invasive brain-to-brain interface (BBI): Establishing functional links between two brains. *PLoS ONE* 8, 4 (Apr. 2013), e60410.
[180] Tianyou Yu, Yuanqing Li, Jinyi Long, and Zhenghui Gu. 2012. Surfing the Internet with a BCI mouse. *J. Neural Eng.* 9, 3 (June 2012), 036012.
[181] Peng Yuan, Yijun Wang, Xiaorong Gao, Tzyy-Ping Jung, and Shangkai Gao. 2013. A collaborative brain-computer interface for accelerating human decision making. In *Proceedings of the International Conference on Universal Access in Human-Computer Interaction*. Springer, Berlin, 672–681.
[182] Lan Zhang, Ker Jiun Wang, Huan Chen, and Zhi Hong Mao. 2016. Internet of brain: Decoding human intention and coupling EEG signals with Internet services. In *Proceedings of the International Conference on Service Science (ICSS'16)*. IEEE, 172–179.
[183] PeiYun Zhang, MengChu Zhou, and Giancarlo Fortino. 2018. Security and trust issues in Fog computing: A survey. *Future Gen. Comput. Syst.* 88 (Nov. 2018), 16–27.
[184] Shaomin Zhang, Sheng Yuan, Lipeng Huang, Xiaoxiang Zheng, Zhaohui Wu, Kedi Xu, and Gang Pan. 2019. Human mind control of rat Cyborg's continuous locomotion with wireless brain-to-brain interface. *Sci. Rep.* 9, 1 (Dec 2019), 1321.
[185] Xiang Zhang, Lina Yao, Shuai Zhang, Salil Kanhere, Michael Sheng, and Yunhao Liu. 2019. Internet of Things meets brain–computer interface: A unified deep learning framework for enabling human-thing cognitive interactivity. *IEEE Internet Things J.* 6, 2 (Apr. 2019), 2084–2092.
[186] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. 2016. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* 104, 9 (Sep. 2016), 1727–1765.

Received November 2019; revised August 2020; accepted September 2020