

# Cybersecurity in Brain-Computer Interfaces: State-of-the-art, opportunities, and future challenges

Sergio López Bernal\*, Alberto Huertas Celdrán†, Gregorio Martínez Pérez \*,  
Michael Taynnan Barros †, Sasitharan Balasubramaniam †

\* Departamento de Ingeniería de la Información y las Comunicaciones  
University of Murcia, 30071 Murcia, Spain  
Email: slopez@um.es, gregorio@um.es

† Telecommunication Software and Systems Group  
Waterford Institute of Technology, Waterford, Ireland  
Email: ahuertas@tssg.org, mbarros@tssg.org, sasib@tssg.org

**Abstract**—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, from medicine to entertainment, the trend of these interfaces is breaking new frontiers enabling new innovative brain-to-brain and brain-to-the-Internet communication paradigms. The increment in the possibilities offered by BCIs generates an attractive terrain for attackers, since users' personal information and physical integrity could be under risk. This article presents a comprehensive work to understand BCIs, their software cybersecurity concerns and future challenges. We initiate the article by reviewing the state-of-the-art of BCIs from the availability, confidentiality, integrity, and safety risks associated with their most well-known classifications. After that, we review the existing architectural versions of the BCI life-cycle and homogenise them in a new approach that overcomes the limitations of the current ones. A survey of the cybersecurity attacks affecting each phase of the BCI cycle is performed to analyse the impacts and countermeasures documented in the literature. Furthermore, new unexplored attacks concerning each phase are presented as well. After that, we review documented cyberattacks affecting the deployments of the BCI cycle, as well as their impacts and countermeasures. Like in the BCI design, missed by the literature, are documented. Finally, we reflect on lessons learned, highlighting research trends and future challenges concerning cybersecurity on BCIs.

**Index Terms**—Brain-computer Interfaces, BCI, cybersecurity, privacy, safety

## I. INTRODUCTION

Brain-Computer Interfaces (BCIs) emerged in the 1970s with the goal of acquiring and processing users' brain activity to later perform specific actions over external machines or devices [1]. After several decades of research, this functionality has been extended by enabling not only neural activity recording, but also stimulation [2], [3]. Fig. 1 describes the general components and processes defining a

common BCI cycle in charge of recording and stimulating neurons. 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 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 Fig. 1). This activity is acquired by the BCI and transformed into digital data (phase 2). After that, data is analysed 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 are able to present optional feedback to the users, which allows the generation of new neural activity. On the other hand, the counterclockwise direction of Fig. 1 starts in phase 4, where applications define the intended stimulation actions to be performed. In phase 3, this action is processed 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 to the technology used, as reviewed in Section II (step 2). In a nutshell, a BCI can be a unidirectional or bidirectional communication system between the brain and external computational devices. Unidirectional communications is when they either acquire data or stimulate neurons, on the other hand bidirectional communications is when they perform both tasks [4].

From the cybersecurity perspective, BCIs are in an early and immature stage. Cybersecurity has not been considered as a critical aspect of BCIs until recent years, where terms such as neurosecurity, neuroprivacy, neuroconfidentiality, brain-hacking, or neuroethics have emerged [5]–[7]. Existing works of the literature have detected certain cybersecurity attacks affecting BCI integrity, confidentiality, availability and safety, but they do not perform a comprehensive analysis and miss relevant concerns [1], [8]–[11]. Furthermore, the expansion

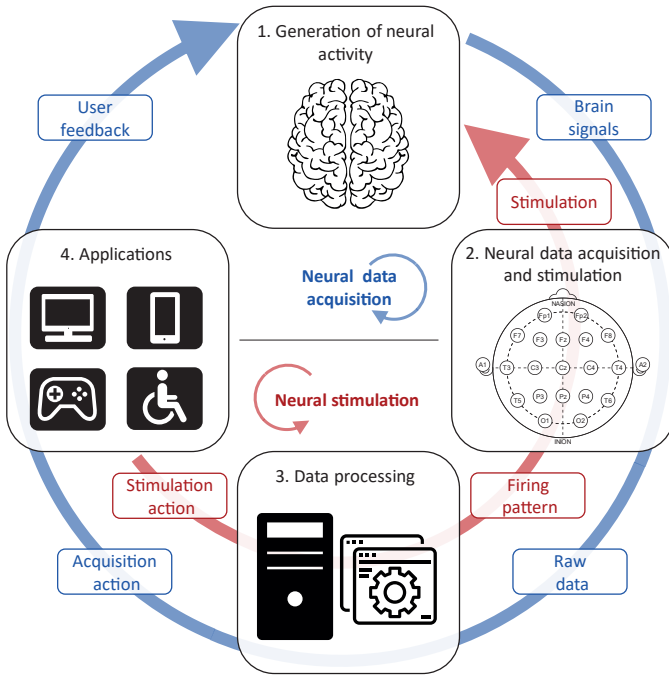


Fig. 1. General functioning of a bidirectional BCI. The clockwise flow indicated with a blue arrow represents the neural data acquisition process, while the counterclockwise flow represented with a red arrow models the brain stimulation.

of BCI to new markets, e.g video games or entertainment, generates great risks in terms of data confidentiality [1], [8], [10], [11]. In this context, users' personal information, such as thoughts, emotions, sexual orientation or religious beliefs are under threats if cybersecurity measures are not adopted [7], [8], [10]. The technological revolution of recent years, combined with movements such as the Internet of Things (IoT), brings an acceleration in the creation of new devices lacking cybersecurity standards and solutions based on the concepts of *security-by-design* and *privacy-by-design* [9]–[12]. This revolution also brings to reality disruptive scenarios such as direct communications between brains, known as Brain-to-Brain (BtB) or Brainets [13]–[16], and brains connected to the Internet (Brain-to-Internet (BtI)), which will require important efforts from the cybersecurity prism.

Once summarised the functioning of BCIs and their cybersecurity status, the scope of this paper lies on analysing the cybersecurity issues of software components that intervene in the processes, working phases, and communications of BCIs. In addition, this work considers the cybersecurity concerns of infrastructures, such as computers, smartphones, and cloud platforms, where different BCI architectures are deployed. It is also important to note that this article does not focus on the physical impacts that cybersecurity threats might have on humans. With the aim of providing an overview of the main topics considered in this work, Fig. 2 shows the distribution of

the 198 works cited by this article. They are classified into four main categories: BCI, Cybersecurity, Network communications, and IoT. Intersections of categories are also considered to provide a better understanding. In summary, as can be seen in the number of references, the article is mainly focused on BCI, Cybersecurity and Network communications.

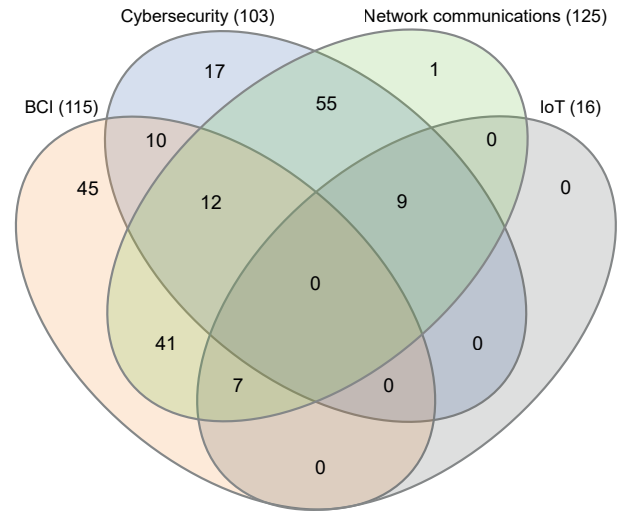


Fig. 2. Classification and distribution of the article references.

Aligned with the aspects described above, to the best of our knowledge, this article is the first work that exhaustively reviews and analyses the BCI field from the cybersecurity and safety points of view. In this context, Section II reviews the most critical risks associated with each particular BCI classification from the data integrity, data confidentiality, data and service availability, and safety perspectives. This classification analysis highlights the most relevant cybersecurity impacts of each BCI family. Once reviewed existing BCI cybersecurity risks, Section III focuses on analysing the cybersecurity issues related to the design of the BCI life-cycle. In this context, firstly we unify the existing heterogeneous BCI life-cycles in a novel and common approach that integrates recording and stimulation processes. It is worthy to comment that before this work, the neural recording process was widely documented, although existing works proposed different phases and responsibilities. Furthermore, the phases of the neural stimulation were completely missing, and no common mechanisms were defined to address bidirectional BCI systems. Once proposed the new life-cycle design approach, Section III reviews the attacks that exploit the cybersecurity risks described in Section II, the impact generated by the attacks and the countermeasures to mitigate them, both documented in the literature and detected by us. After highlighting the cybersecurity issues related to the BCI design, Section IV reviews the inherent cyberattacks, their impacts and countermeasures affecting to current BCI deployments scenarios. This section identify the cybersecurity issues generated by the devices implementing the responsibilities

of each life-cycle phase, as well as the communication mechanisms and the application scenarios. The last main contribution of this article is provided by Section V, where we give our vision regarding the trend of BCI and the cybersecurity challenges that this evolution will generate in the future. Finally, Section VI presents some conclusions and future work.

## II. CYBERSECURITY RISKS ASSOCIATED WITH BCI CLASSIFICATIONS

This section analyses the cybersecurity risks of the most well-known BCI classifications found in the literature, defining a risk assessment over each category of BCI and being the first work focusing in that aspect. At this point, it is worthy to note that solutions combining aspects from several families usually result in the aggregation of their risks. Finally, this section documents the cybersecurity concerns generated from the risks according to the following common aspects considered in cybersecurity:

- *Integrity*: protection of users neural and private data in such a way that it cannot be manipulated between sender and receiver,
- *Confidentiality*: restrictions over the data to ensure its accessibility only for authorised users,
- *Availability*: guarantee over a service or the management of its data to ensure that there will be no alteration in its correct functioning,
- *Safety*: preservation of the the physical integrity of the user, not being negatively affected by the use of the system.

### A. Design of BCIs

The design of BCIs decides who is responsible for initiating the neural data acquisition process and how the process is performed. In other words, this classification indicates if the process is triggered by the user or the BCI, and how the interaction is done to perform the intended actions [12], [17]–[20]. According to this categorisation, four BCI families have been defined in the literature: active, passive, reactive, and hybrid. From the cybersecurity perspective, the main risks found for these four BCI families are adversarial attacks, as explained in the following paragraphs.

In active BCIs, also known as independent [18] or spontaneous [12], users intentionally initiate a predefined action that generates brain activity, such as imaging limb movements, which is then captured by the BCI [18], [19]. An example of an action is the imagination of limbs movements [18]. Active BCIs have been used by Gilja et al. [21] for the control of a computer cursor in rhesus monkeys. Passive BCIs, in contrast to active BCIs, focus on the acquisition of spontaneous and non-evoked brain activity, typically generated during complex real-world tasks, such as the actions performed by a pilot during a flight [17], [19].

Passive BCIs have been used to measure mental states such as attention, stress, workload or emotions [22]. The third family is termed Reactive BCIs, also identified as dependent [18] or evoked [12]. This family depends on external stimuli presented to the users and the neural responses generated by their brains as a response. Reactive BCIs are used, for example, to detect situations in which the user recognises external stimuli from a set of unknown. Finally, Hybrid BCIs can be considered from two perspectives. On the one hand, they are BCI systems that receive different types of brain signals as input [18]. Focusing on this approach, Ramadan et al. [12] and Hong et al. [20] showed different possibilities and their purpose. For example, a combination of Electroencephalography (EEG) and Electromyography (EMG) to improve accuracy and enhance application performance. On the other hand, Wahlstrom et al. [17] defined hybrid BCIs as a combination of, at least, one active, passive or reactive BCI system with non-BCI technologies to improve system performance (e.g. combination of an active BCI and a finite state automaton to control a robot).

Regarding the cybersecurity risks of the previous BCI families, we identify malicious external stimuli as the most damaging one. They are exploited by adversarial attacks, explained in Section III-A and III-D, which are based on presenting malicious inputs either to the user or the BCI to obtain a benefit. An example of this benefit is the use of subliminal visual stimuli to generate specific brain signals that imply sensitive data leakage, such as the acquisition of thoughts or personal beliefs. In this context, Wahlstrom et al. [17] indicated that if users with active BCIs are able to stop the BCI functioning and they have given consent for the acquisition of such data, there is no risk of confidentiality attacks. However, we identify that adversarial attacks applied to these BCIs generate data confidentiality concerns, as the previous conditions do not prevent BCIs from suffering vulnerabilities. In addition, Wahlstrom et al. documented that passive BCIs are at risk of data confidentiality attacks, since users do not have control over the BCI. Moreover, they highlighted that in reactive BCIs confidentiality issues are unlikely to arise if the neural activity is filtered, users are in a controlled environment, and they gave their consent. In contrast, adversarial attacks, based on the subliminal visual principles mentioned above, have been detected in the literature [8], [23]. Related to hybrid BCIs, Wahlstrom et al. [17] identified that the risk of these technologies are the combination of the risks of each of their parts. Taking into account these aspects, we also detect data integrity and data availability concerns in all BCI designs, since adversarial attacks can derive in the alteration of the data acquired by the BCI or even the disruption of the data acquisition process. In addition, we identify safety issues generated from these problems. Based on the above concerns, we consider that hybrid BCIs have the highest risk, followed by reactive BCIs, passive BCIs, and finally active BCIs.

Fig. 3 summarises the risks described in this classification. Each family has been represented by a line colour, while the risks documented in this section have been indicated by a number. Based on that, the severity of these risks has been considered based on four different types of impacts (integrity, confidentiality, availability and safety), represented in the vertex of each radar chart. This severity is quantified in a scale between zero and three, where a zero value defines an absence of risk, and three represents a critical high risk.

### B. BCI technology

BCIs are also differentiated according to their technology, where two additional sub classifications arise depending on if they are intended for acquiring neural data or for brain stimulation. Taking into consideration the acquisition of brain waves, the most representative technologies are EEG, Functional Magnetic Resonance Imaging (fMRI), Magnetoencephalography (MEG), Electroencephalography (EEG), and neural dust [12], [18], [24], [25]. On the other hand, focusing on brain stimulation techniques, the most relevant ones are Transcranial Magnetic Stimulation (TMS), Transcranial Electrical Stimulation (tES), Transcranial Focused Ultrasound (tFUS), Deep Brain Stimulation (DBS), and neural dust [3], [26]. All these families generate cybersecurity risks, where we detect issues related to their temporal and spatial resolution. In addition, the inherent risks associated with acquisition and stimulation technologies are also considered by this classification in the next paragraphs.

Related to neural activity recording, Electroencephalography (EEG) is a non-invasive technology that uses electrodes placed on the scalp [12]. This technology highlights for being easy to use, cheap, portable and with a high temporal resolution (in the order of milliseconds) [12], [24]. It is the most widely used non-invasive technology, mainly in video games and entertainment [25], [27]. However, it has poor spatial resolution and the acquired brain waves can be distorted by other neural activity, such as the movements of muscles and eyes, known as artifacts [24]. Functional Magnetic Resonance Imaging (fMRI) is another non-invasive technology used to measure the variation of blood haemoglobin concentrations during brain activity. It has better spatial resolution than EEG and Magnetoencephalography (MEG), so it can identify active zones throughout the brain. However, it has a poor temporal resolution, between 1 and 2 seconds [12], [18], [24]. The resolution of fMRI is also affected by head movements [12]. This technology is useful as a in clinical scenarios to treat neurological conditions such as stroke or mental disorders, although it is not applicable to everyday use [18]. Continuing with non-invasive recording technologies, MEG uses functional neuroimaging over magnetic fields produced by the electric current generated by cortical neurons. This method has great temporal and spatial resolution. Despite these benefits, MEG can only be used in magnetically shielded installations, and it is not portable. This technology is widely used for the detection of regions

with abnormal brain functions and in tetraplegic and stroke patients [12], [18]. Finally, Electroencephalography (EEG) is a partial-invasive method in which a grid of electrodes is placed on the surface of the brain [18]. It offers a Signal-to-Noise Ratio (SNR) superior to non-invasive systems, such as EEG, as well as higher spatial and temporal resolution. In addition, it allows better detection of high frequency oscillatory activity [24]. Despite the above advantages, EEG cannot be used to detect single-neuron spikes [18] and it is very challenging to use these devices outside an operating room [12].

Regarding the stimulation of neurons, Transcranial Magnetic Stimulation (TMS) is a technology that generates electrical fields within the brain, reaching the cortex, and aiming to modulate brain activity and behaviour. This technology has obtained FDA approval in 2018 to treat depression and headaches [3]. TMS has also been used for testing dynamic communication between interconnected areas of the brain [26] and cognitive ageing [28]. Although TMS has a good temporal resolution, it presents a bad spatial precision [18]. Transcranial Electrical Stimulation (tES) is another stimulation technique that uses weak, painless currents applied to the scalp [26]. It can be based on Direct Current Stimulation (tDCS) or Alternating Current Stimulation (tACS). tDCS is a simple method that stimulates the cortex and affect relatively large areas, presenting a low spatial and temporal resolution. In contrast, tACS present a good temporal precision [26]. It has been reported that tES can enhance and perturb cognitive processes, such as creative problem solving or working memory, when applied to different brain regions. Furthermore, it can be used to improve working memory performance and motor behaviour [3], [26]. Although these technologies are promising, they are not mature enough for its use in humans, in terms of reliability and reproducibility [3], [29]. Transcranial Focused Ultrasound (tFUS) is a novel neuromodulation technique that offers a high spatial resolution, being the only non-invasive technology able to penetrate the skull and stimulate specific circuits deep in the brain [30], [31]. It has been used to stimulate the activity of cortical, thalamic and hippocampal circuits in animals [3] and it may be useful to identify and treat neurological and psychiatric disorders in humans, such as neuropathic pain or depression, due to its potential to induce plastic changes in aberrant brain circuits [31]. Finally, Deep Brain Stimulation (DBS) is an invasive neurostimulation technique that involves a surgical procedure for implanting electrodes deep within the brain. This invasiveness provides DBS with good spatial and temporal resolution. Focusing on its functioning, the implanted device sends electric currents into targeted subcortical areas to increase, suppress or distort neural activity. This method has been used for the treatment of conditions such as Parkinson disease, dystonia and chronic pain syndromes [2], [5], [7], [31]. Despite the benefits of DBS, the associated surgeries required may have complications such as infection or haemorrhage [31].

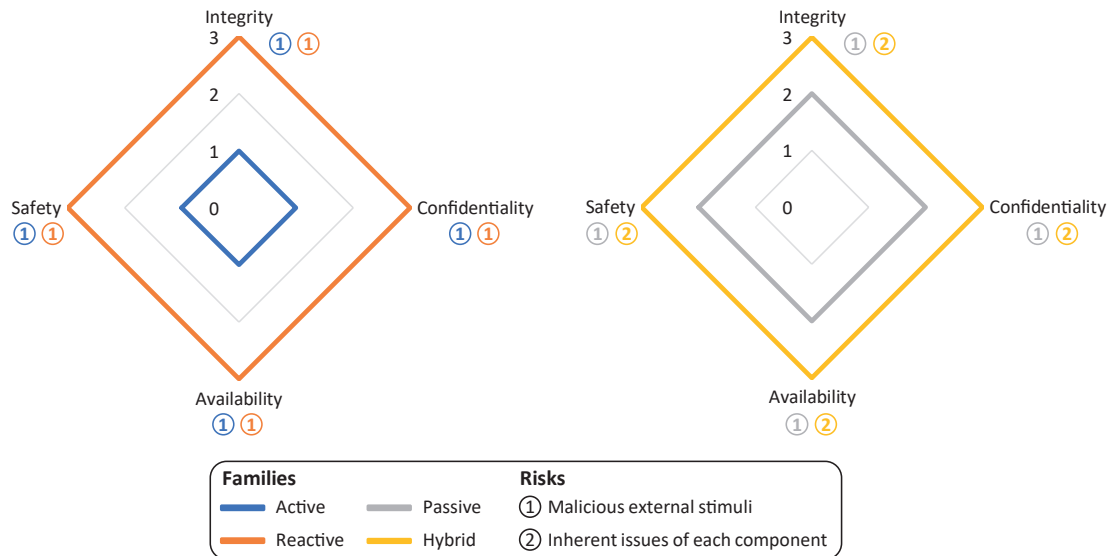


Fig. 3. Cybersecurity and safety risks associated with the design of BCIs.

Neural nanonetworks comprise several technologies to record and stimulate neural activity through the use of nanodevices. In particular, neural dust is a solution to acquire neural data relying on nanodevices allocated into the cortex, beneath the skull and below the dura mater [18], [32]. An interrogator is powered by an external transceiver using radio frequency power transfer [32], and it establishes wireless power and communication with the neural dust using ultrasounds [32], [33]. This nanotechnology offers some advantages, as it does not use microelectrode shafts that can damage the nervous tissue, it records very concrete areas within the brain and it can work as a closed-loop system based on real-time adaptation, offering high spatial and temporal resolution [18]. It is also an interesting alternative to electromagnetic systems due to its lower attenuation and higher efficiency [33]. Wirdatmadja et al. [34] used the neural dust model defined by Seo et al. [32] to propose a stimulation system based on optogenetic nanonetworks and the definition of different firing patterns (e.g. brain regions, frequencies, temporal synchronisation) to interact with the devices. Zheng et al. [35] developed an implantable device based on optogenetic stimulation for peripheral nerves, focused on activating limb muscles. Lee et al. [36] defined the concept of *Neurograin* sensors, implementing a network of nanodevices that uses wireless energy harvesting, and validated in both *ex vivo* and *in vivo* rodent tests. Despite the advantages of these technologies, they are experimental and they have not yet been tested in humans [18].

Once summarised the main aspects of the families making up this classification, we identify that both temporal and spatial resolutions generate important cybersecurity risks, as in Section II-C. In particular, BCI technologies such as DBS, neural dust, ECoG or MEG present higher risks

in terms of data confidentiality and safety that those with lower resolutions, like EEG, fMRI or TMS. In addition, it is important to highlight that the invasiveness of these methods also impacts on the severity of the risks associated with each family. Because of that, DBS and neural dust have a higher risk than ECoG due to their invasiveness, and all of them are more damaging than MEG, as it is a non-invasive technology. In contrast, technologies with low resolutions present concerns on data and service availability, since they transmit a reduced amount of data that can be affected more easily by electromagnetic interference. According to the inherent functioning of acquisition and stimulation systems we detect two more risks. On the one hand, since acquisition technologies aim to record neural data, they generate risks in terms of data integrity and confidentiality, where attacks can aim to impersonate or gather users' neural data. On the other hand, stimulation systems mainly present safety issues, where attackers can cause brain damage. Several works in the literature review the safety concerns of stimulation technologies. According to Glannon et al. [37], ECoG has a risk of infection and haemorrhage, and the micro electrode arrays used present potential problems of bio compatibility with neural tissue. In addition, Polanía et al. [26] indicated that TMS pulses applied to particular areas can induce suppression of visual perception or speech arrest, which serve as an opportunity for attackers. Finally, we identify electromagnetic noise as a risk directed over the physical aspects of non-invasive transmission systems. In particular, technologies such as EEG acquire electrical currents, while fMRI and MEG acquire magnetic fields emitted from the brain. These specific aspects can serve as an opportunity for attackers to override the legitimate information generated by the brain, creating concerns in terms of data integrity and availability. These attacks are explained in Section III-A.

Finally, Fig. 4 indicates the risks that affect each of the BCI technologies documented in this classification. It is important to note that the risks associated with the precision and electromagnetic noise are also influenced by the level of invasiveness of these technologies. Because of that, invasive systems offer higher risks than non-invasive systems.

### C. Level of Invasiveness

The level of invasiveness indicates whether the BCI device is implanted in the user's body, or placed externally. This classification has been widely studied in the literature [1], [7], [9], [11], [12], [17], [18], [23], [24], [26], [38]–[40], where the following three families have been proposed: invasive, partial-invasive and non-invasive. In the following paragraphs, we give an overview of the previous three families and highlight their main discriminant characteristics: the spatial and temporal resolution to record and stimulate neural activity, and the intrusiveness affecting persons' physical safety. Finally, for each family we detect the cybersecurity concerns related to the previous characteristics.

Invasive systems require a neurosurgery process that involves opening the scalp, the skull and placing in the brain tissue the BCI components to record or stimulate neurons. This technology has been used mainly in the medical field because it allows measuring neural activity with very little noise. In the last decades, they allow direct interaction with the brain, enabling the stimulation of individual neurons [18], [34]. The second family of this category is called partial-invasive and the BCIs components are placed on the brain surface, without penetrating the nervous tissue. This family is used in the field of medicine, for example, with subdural electrodes aiming to identify the location of epileptic seizures [24], [41]. This type of BCI has lower temporal and spatial resolution than the previous one, which affect to its applicability in some application scenarios. Finally, non-invasive BCIs are applied outside the skull, directly on the scalp. They present lower temporal and spatial resolution than the previous two families due to the attenuation and filtered provoked by the bone and skin. However, they have an important role in the health field, where non-invasive neural stimulation systems are gaining popularity [12]. In addition, these technologies are nowadays the most extended systems due to their simplicity and applicability in entertainment scenarios, where final users are benefited from their advantages [1], [12].

Analysing the previous three families from the cybersecurity point of view, we have identified that two of the most serious risks are the temporal and spatial resolution. In this context, BCIs with higher spatial resolution can access to more precise neural data or stimulate more specific brain regions than those who have lower precision [12], [18]. In addition, a high temporal resolution allows attackers to perform more complex attacks since the communication delay is reduced. In this context, invasive systems have access to neural-level

data, whereas less invasive systems acquire aggregated data with less resolution. That increase of precision generates concerns in terms of data confidentiality, where systems with higher resolution have access to more precise and detailed information (e.g. thoughts or beliefs). In addition, BCIs precision can impact users' physical safety, where a high precision can increase the damage of attacks during neurostimulation processes. However, a reduction of the precision derives in the transmission of a reduced quantity of data that can be insufficient for the correct functioning of BCIs in specific scenarios, impacting service availability. The level of intrusiveness is another risk detected in the literature. Invasive and partial-invasive BCIs are at risk of tissue damage, infection and rejection due to the surgical procedure required to place them [1], [12], [18], [42]–[44]. In addition, both present a risk of degradation in the acquisition and stimulation technologies used, such as electrodes, when used for a long period of time [42].

Focusing on temporal and spatial resolution, invasive systems have the highest risk within these criteria, followed by partial- and non-invasive BCIs. Invasive systems introduce more serious concerns in terms of user's physical integrity than partial-invasive, while non-invasive BCIs are immune to them. However, non-invasive stimulation systems significantly reduce, but not suppress, safety risks [26]. At this point, it is important to highlight that the majority of attacks on BCIs have been conducted over non-invasive systems. However, it is motivated by their designs and implementations, and not due to problems inherent to the level of invasiveness. Finally, Fig. 5 represents the risks detected for this BCI classification.

### D. Synchronisation

This classification is focused on the interaction between the BCIs and the users. It determines who controls the recording and stimulation processes and in which time slots. Based on that, two families of BCIs have been documented in the literature [12], [45]: synchronous and asynchronous. The next paragraphs of this section highlight the most important aspects of these families, as well as the the risks and concerns detected for this classification, being the control the communication between BCIs and users the most critical aspect.

In synchronous (or cue-paced) BCI systems, the interaction between the user and the BCI takes place during specific periods of time [12]. This planning is imposed by the BCI, which controls the communication. Outside these periods, the BCI is not able to communicate with the user. They are easier to implement than asynchronous BCIs, but they are not suitable for acquiring users' mental intentions [45]. Bentabet et al. [46] used synchronous BCIs to control domotic devices, extracting features from P300 waves. In contrast, in asynchronous (or self-paced) systems, users can generate brain signals at any time, and the BCIs will react to these events. Ramadan et al. [12] highlighted the complexity of detecting

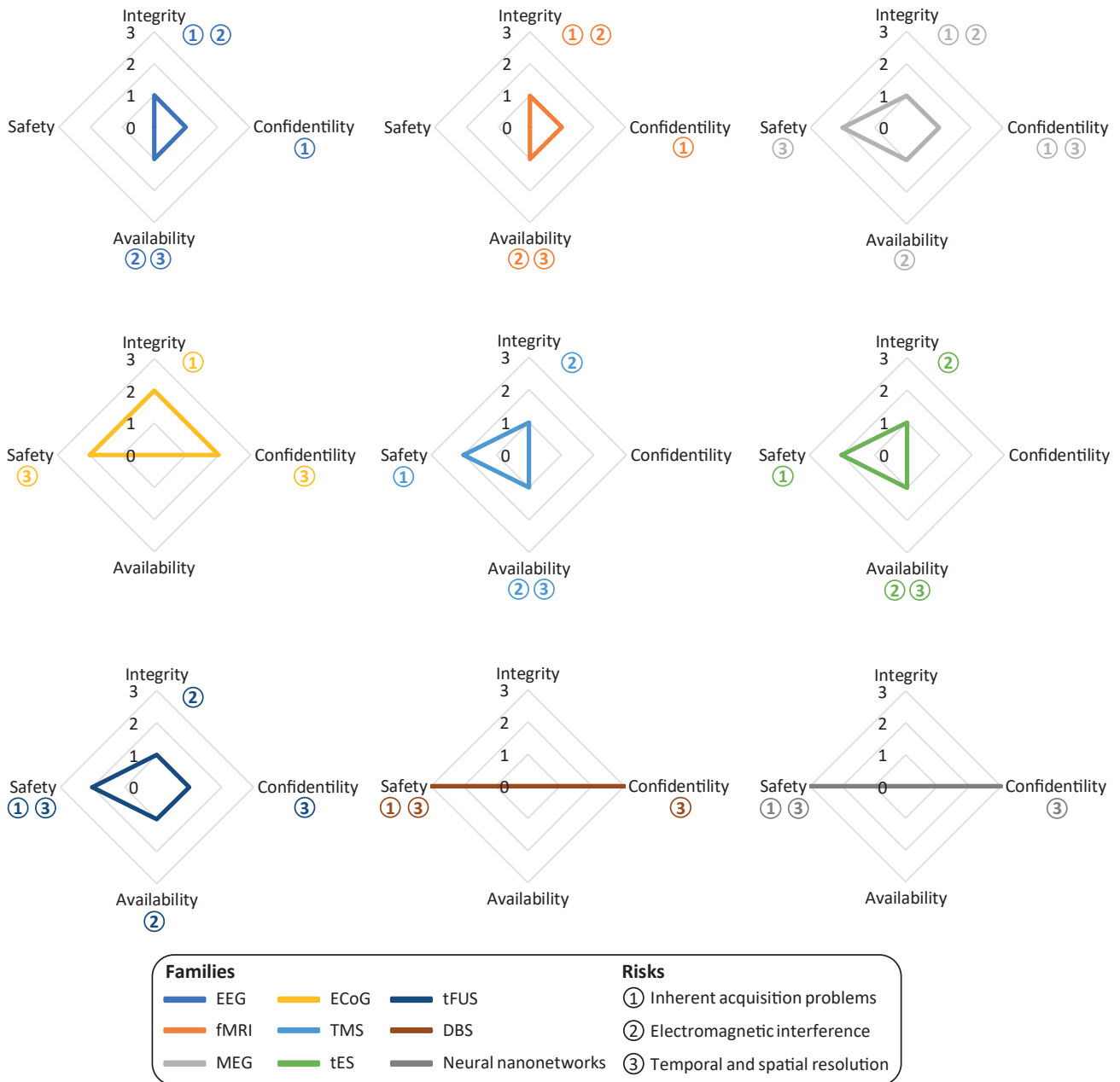


Fig. 4. Cybersecurity and safety risks associated with the BCI technology.

idle states, and proposed the use of a button to activate or deactivate the acquisition of stimuli. An et al. [45] proposed the design of an asynchronous BCI to control a virtual avatar in a game. In this game, the avatar competes with other users in a race, running continuously and, when a control command is received, an action on the avatar is performed. As can be seen, these systems depend on the moment and the action performed by the user, without control imposed from the BCI.

Considering the cybersecurity risks generated by these two families of BCIs, no risks have been documented in the literature. However, we identify that their main issue

is a loss of the control over the communication between a BCI and its user. In this context, we detect that synchronous BCIs, which control the communication, originate data integrity and confidentiality concerns, where attackers taking control over the BCI are able to gather and alter the neural data. In addition, availability issues are possible, where attackers disable the data acquisition process, even without the knowledge of the users. Finally, this lack of control can generate safety impacts, where attackers managing the functionality of a BCI can produce critical physical harm, such as malicious movements of a wheelchair or damaging stimulation patterns. On the other hand, since asynchronous

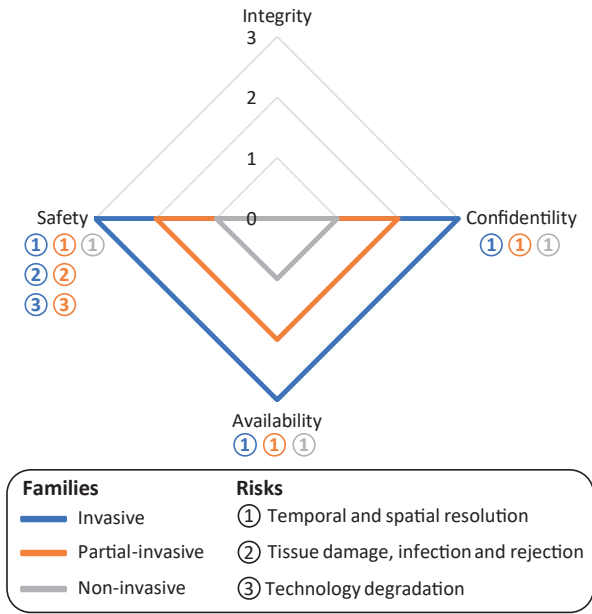


Fig. 5. Cybersecurity and safety risks associated with the invasiveness of BCIs.

BCIs have less decision capabilities and awareness over the acquisition process, we identify that this BCI family has a risk of malicious external stimuli aiming to perform adversarial attacks, as reviewed in Section III-A. These stimuli originate concerns in terms of data integrity, where attackers impersonate the neural data generated that is communicated to the BCI. Moreover, they generate data and service availability issues, since these stimuli can impact the acquisition process and thus the normal functioning of the communication. Finally, we consider that asynchronous BCIs have a high risk of confidentiality problems, where the BCIs are constantly acquiring brain activity and therefore sensitive information is gathered. The previous attacks and concerns also generate safety problems.

Taking into consideration the above, asynchronous BCIs present greater data integrity and availability issues, due to their larger temporal exposition to neural data. However, considering the awareness and control capabilities of the user over the communication, synchronous BCIs have higher concerns over both issues. In addition, although both synchronous and asynchronous BCIs share common concerns, we detect that the first family has a higher risk, since attacks over BCIs are more probable than those based on user neural data impersonation. This situation is summarised in Fig. 6, which highlights the difference of severity between these BCI families.

### E. Usage Scenario

The usage or application scenario is another well-known criteria to classify BCIs. It was proposed by Li et al. [1] and they highlighted the following four types: neuromedical, user authentication, gaming and entertainment, and smartphone-

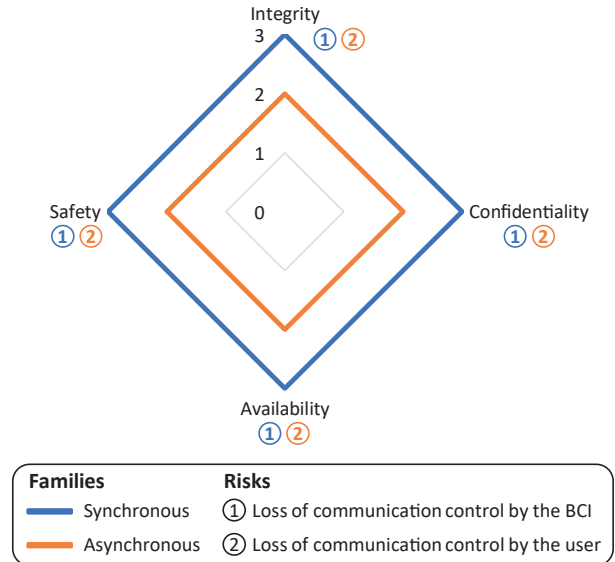


Fig. 6. Cybersecurity and safety risks associated with the synchronisation of BCIs.

based BCIs. The cybersecurity risks associated with this classification strongly depend on the characteristics and actions took by each family or scenario. After summarising the main aspects of this classification the risks detected for each family will be commented and explained in the subsequent paragraphs.

The field of neuromedical applications has been the centre of the research in BCIs for decades. The applications developed within this field range from the control of prosthetic limbs and wheelchairs [1], [5], [7] to the use in brain stimulation procedures [18], [26], [34]. In addition, Chaudhary et al. [47] used BCIs to establish a simple communication system with completely paralysed patients. Nowadays, current research on BCIs focuses on novel mechanisms and technologies to analyse and stimulate the brain, (considered in Section V). The second scenario is the use of BCIs as authentication systems. The authentication process consists in recording the user's brain waves while performing a previously established task. Then, the acquired neural data is validated against the entity, which contains the authentication data to validate the user. BCI is a good biometric element since each brain generates unique patterns [9]–[11], [48], [49], and the mental action that triggers the authentication process can be modified enabling an adaptive and flexible authentication mechanism. Finally, brain signals can be easily affected and it is difficult to reproduce them under the effects of stress, anxiety or drugs [8]. The third type, gaming and entertainment, arose due to the utility of BCIs in the video game industry. Thus, development tasks have been facilitated by the use of common APIs. Ahn et al. [25] did a review of BCI games, highlighting games such as Bacteria Hunt, and a survey involving researchers,



game developers and users. McMahon et al. [27] focused on virtual reality (VR) and created a low-cost open-source development environment prototype for BCI games. Finally, the smartphone-based BCIs are based on the relationship between BCIs and user applications stored in smartphones, where it is the most common usage scenario in commercial BCI brands [10]. This usage scenario is described in Section IV-A.

The cybersecurity risks of each BCI family vary considerably according to the usage scenario. These risks generate data confidentiality concerns in medical scenarios, where attackers are able to gather sensitive information [1], [50]. Moreover, they are at risk of user's physical harm, since BCIs are used to improve health conditions in patients. Denning et al. [5] identified safety concerns based on malicious neural stimulation actions, whereas Li et al. [1] detected issues on service integrity if users modify the parameters that control prosthetic limbs to gain a personal benefit. In addition, we identify that neuromedical scenarios have a risk on the management of very sensitive information of patients, such as their personal data, medical history and neural activity data, affecting users' confidentiality. Regarding authentication scenarios, Li et al. [1] identified data confidentiality concerns based on the acquisition of the authentication data. In addition, we detect that they are at risk of malicious external stimuli aiming to alter the neural data used for the authentication process and thus impact on the data integrity and availability. On the other hand, we identify that the gaming and entertainment scenario has a risk of malicious external stimuli, as this family is based on audiovisual systems that serve as an opportunity for attackers to perform adversarial attacks. Because of that, we highlight data confidentiality issues, where attackers present malicious stimuli to acquire sensitive data taking advantage of these multimedia resources. This situation also affects data integrity and availability, as explained in Section III-A. Finally, smartphone-based scenarios present several risks. First, they rely on systems with potential problems, such as a lack of updates of the Operating System (OS) and applications [1], [8], [11], [39]. In addition, we detect that the heterogeneity of the hardware, OSs, applications used and versions of each specific smartphone can also produce cybersecurity risks [51]. Based on that, Takabi et al. [10] analysed several smartphone applications developed with the NeuroSky platform [52]. They detected that some third-party applications required access to the phone book and permissions to read the call logs, which was not the objective of the applications, generating confidentiality concerns. Moreover, we identify that this lack of control over the elements of the smartphone generates concerns in terms of data integrity, data availability and safety, where attackers perform malicious actions over the users and their data.

In conclusion, Fig. 7 provides an overview of the previous concerns. The highest risks of neuromedical scenarios

are on integrity, confidentiality and safety issues, due to their inherent critical actions. For authentication systems and gaming and entertainment scenarios, we consider that integrity, confidentiality and availability concerns are equally probable. Finally, smartphone-based scenarios present all four concerns. On the other hand, TABLE I groups all the information described in the section. It indicates, for each classification and BCI family, the general references that treat relevant concepts associated with each BCI family. In addition, the four concerns analysed throughout the section are exposed (i.e. integrity, confidentiality, availability and safety), where one or more references indicate that the BCI family presents a concern previously documented in the literature. Moreover, our contribution is indicated with a red icon (✗). Finally, a green icon (✓) indicates that there are no concerns identified.

### III. CYBERATTACKS AFFECTING THE BCI CYCLE, IMPACTS AND COUNTERMEASURES

This section reviews the different operational phases of BCIs detected in the literature, known as BCI cycle, and homogenises them in a new approach that overcomes the existing limitations, shown in Fig. 8. After that, we survey the cybersecurity attacks affecting each phase of the cycle, their impacts, and the countermeasures documented in the literature. Unexplored opportunities in terms of cyberattacks and countermeasures affecting each phase are presented as well.

Different configurations of the BCI cycle have been proposed in the literature. However, the existing versions only consider the signal acquisition process, missing the stimulation of neurons. These solutions present heterogeneous classifications of the BCI cycle, as some of them do not consider the generation of brain signals as a phase or group several phases in only one, without providing information about their roles [7], [48]. Other solutions, as the proposed in [1], [7], [22], [24] 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], [25], [48], [56] while others deal with the concept of *commands* sent to external devices [9], [11], [20], [38]–[40], [46]. In addition, just a few works define the feedback sent by applications to users [1], [7], [9], [11], [24], [38]–[40], [46]. With the goal of homogenising the BCI cycle and addressing the previous missing or confusing points, we present a new version of the BCI cycle with five phases (with clear defined tasks, inputs and outputs) that considers both acquisition and stimulation capabilities. Fig. 8 represents our proposal, where 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.

TABLE I  
CYBERSECURITY RISKS AND CONCERNS BASED ON BCI CLASSIFICATIONS, DIFFERENTIATING BETWEEN THOSE FAMILIES THAT HAVE A LACK OF CYBERSECURITY ISSUES (✓) AND THOSE WITH IDENTIFIED PROBLEMS, EITHER DOCUMENTED IN THE LITERATURE (LIST OF REFERENCES) OR DETECTED BY US (✗).

| BCI classification                      | BCI family               | Family-related literature                     | Cybersecurity concerns |                 |              |        |
|---|--------------------------|---|------------------------|-----------------|--------------|--------|
|   |                          |   | Integrity              | Confidentiality | Availability | Safety |
| Design of BCIs<br>(Section II-A)        | Active                   | [12], [17]–[19], [21]                         | ✗                      | ✗               | ✗            | ✗      |
|   | Passive                  | [17]–[19], [22]                               | ✗                      | [17]            | ✗            | ✗      |
|   | Reactive                 | [8], [12], [17], [18]                         | ✗                      | [8], [23]       | ✗            | ✗      |
|   | Hybrid                   | [12], [17], [18], [20]                        | [17]                   | [17]            | [17]         | [17]   |
| Level of invasiveness<br>(Section II-C) | Invasive                 | [12], [18], [34]                              | ✓                      | ✗               | ✗            | [42]   |
|   | Partial-invasive         | [24], [41]                                    | ✓                      | ✗               | ✗            | [42]   |
|   | Non-invasive             | [1], [12]                                     | ✓                      | ✗               | ✗            | [26]   |
| Synchronisation<br>(Section II-D)       | Synchronous              | [12], [45], [46]                              | ✗                      | ✗               | ✗            | ✗      |
|   | Asynchronous             | [12], [45]                                    | ✗                      | ✗               | ✗            | ✗      |
| Usage scenario<br>(Section II-E)        | Neuromedical             | [1], [5], [7], [18]<br>[26], [34], [47]       | [1]                    | [1], [50]       | ✓            | [5]    |
|   | User authentication      | [1], [8]–[10]<br>[11], [48], [49], [53], [54] | ✗                      | [1]             | ✗            | ✓      |
|   | Gaming and entertainment | [1], [25], [27]                               | ✗                      | ✗               | ✗            | ✓      |
|   | Smart-phone based        | [1], [9], [10], [39]                          | ✗                      | [10]            | ✗            | ✗      |
| BCI Technology<br>(Section II-B)        | EEG                      | [12], [24], [25], [27]                        | ✗                      | ✗               | ✗            | ✓      |
|   | fMRI                     | [12], [18], [24]                              | ✗                      | ✗               | ✗            | ✓      |
|   | MEG                      | [12], [18]                                    | ✗                      | ✗               | ✗            | ✗      |
|   | ECoG                     | [12], [18], [24], [55]                        | ✗                      | ✗               | ✓            | [37]   |
|   | TMS                      | [3], [26], [28]                               | ✗                      | ✓               | ✗            | [26]   |
|   | tES                      | [3], [26], [29]                               | ✗                      | ✓               | ✗            | ✗      |
|   | tFUS                     | [3], [30], [31]                               | ✗                      | ✗               | ✗            | ✗      |
|   | DBS                      | [2], [5], [7], [31]                           | ✓                      | ✗               | ✓            | [31]   |
|   | Neural dust              | [18], [32]–[34]                               | ✓                      | ✗               | ✓            | ✗      |

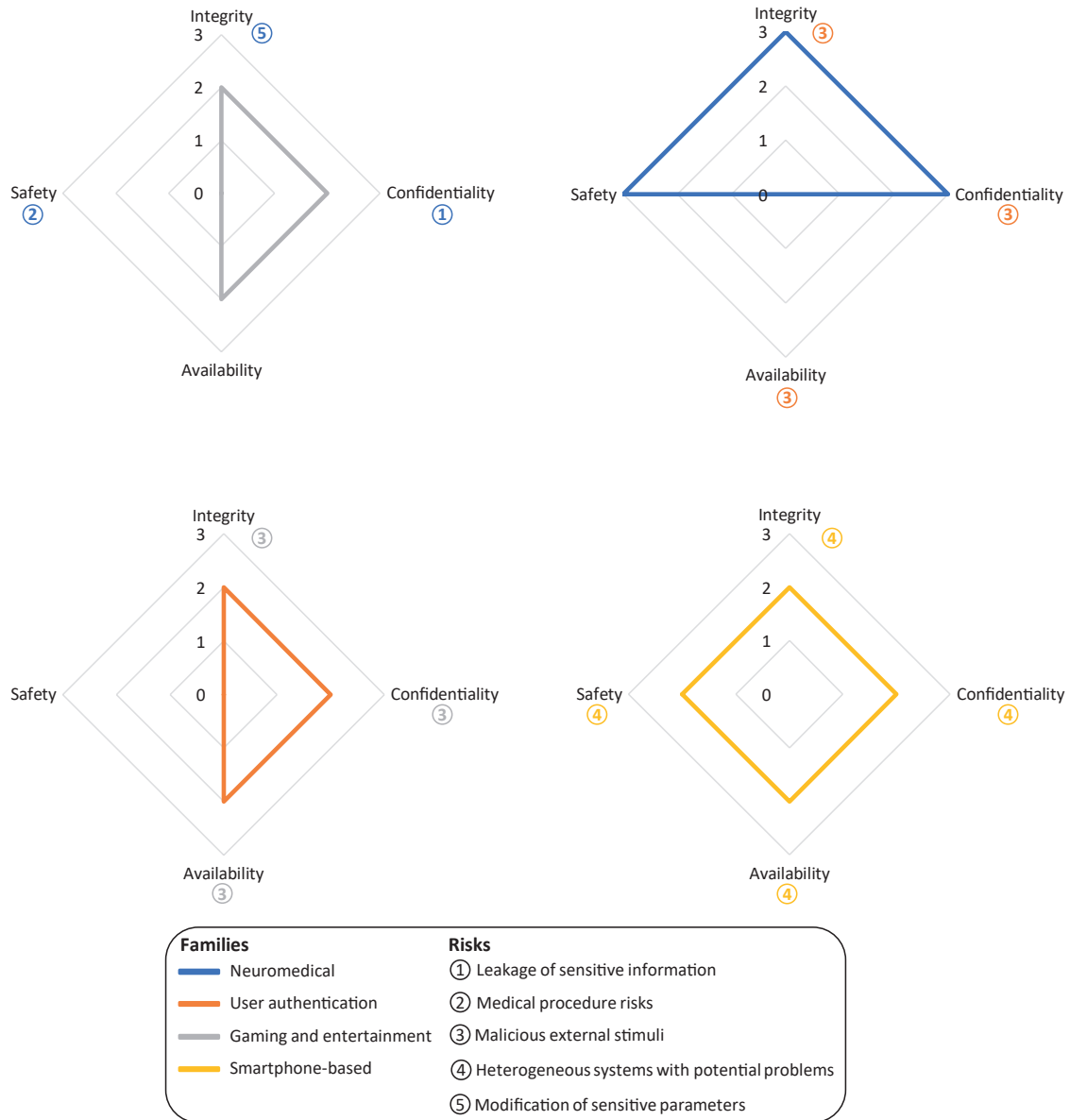


Fig. 7. Cybersecurity and safety risks associated with the BCI usage scenario.

According to the neural acquisition process (clockwise direction in Fig. 8), 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 EEG, fMRI, and so on. Raw analog signals containing the user's intention are then transmitted to phase 3, where a data processing and conversion are required. Specifically, an analog-to-digital conversion procedure is performed to allow further processing of the data. One of the main goals of this phase is to maximise the SNR, which compares the level of the target signal to the level of background noise, to obtain the original

signal as accurately as possible. After that, phase 4 processes the digital neural data to decode the intended action by the user. To perform this task, relevant features are calculated and selected from the neural data. After that, different models (classifiers, predictors, regressors, etc.) or rule-based systems are used to decide the intended action [40], [56]. The action is finally sent to applications in phase 5, where the action is performed. 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 Fig. 8), the loop starts in phase 5, where it is specified the stimulation action in a general way (e.g. stimulate a concrete brain region to treat Alzheimer's disease). This

intended action is transmitted to phase 4, where this input is processed using 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 is intended to transform the firing pattern received, indicated in a general fashion, to specific parameters related to the BCI technology used. For example, the definition of which neurons must be stimulated or the power and voltage required for the process. These stimulation parameters are then transmitted in phase 2 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, that 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 Fig. 8 to the other.

Focusing on the attacks, impacts and countermeasures described later in this section, they have been represented in Fig. 9. As can be seen, each attack has been represented by a colour, which associates the impacts that it generates and the countermeasures to mitigate it. For each impact included in the figure, a simplified version of the BCI cycle is included. Those phases of the cycle marked in red indicate that the impact has been detected in the literature for that specific phase, whereas the blue colour indicates that the impact is our contribution to the phase. In addition, the attacks, impacts and countermeasures marked with references have been proposed in the literature, while those without references are our contribution. Finally, 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.

#### A. Phase 1. Brain signals generation

This first phase of the cycle focuses on the brain processes generating neural activity, which can be influenced by external stimuli. Focusing on the attacks documented for this stage, *adversarial attacks* [57], [58] have been detected in the literature as a mechanism to alter the brain signals generation by presenting intentionally crafted inputs to the system with the goal of disrupting its normal functioning. In this context, these attacks are also an opportunity for attackers trying to disrupt or alter BCI systems that use ML techniques, as explained in Section III-D. To understand the attacks on this phase, it is important to introduce the concept of *Event Related Potential (ERP)*, which is a neurophysiological response to a cognitive, sensory or motor stimulus, detected as a pattern of voltage variation [48]. *P300* is an ERP detected as an amplitude peak in the EEG signal about 300ms after the stimulus and is extensively used due to its quick response [59].

Martinovic et al. [8] used the P300 potential to obtain private information from test subjects and demonstrated attacks on confidentiality. To do this, visual stimuli were presented in the form of images, grouped as follows: 4-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. This study was conducted with 28 test subjects, 18 male and 10 female, using the Emotiv EPOC 14-channel headset [60], a commercial BCI EEG device. The experiment showed 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. [23] demonstrated the possibility of performing subliminal stimuli attacks against data confidentiality. 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 was performed with EEG devices of the brands NeuroSky [52] and Emotiv [61]. We consider that the previous works are important to highlight the importance of cybersecurity in BCI and additional experiments with a higher number of users are required.

Some well-known methods to present stimuli to users and analyse their neural response have been documented in the literature [8], [9], [11]. For example, to analyse with a polygraph the neural activity generated after a question in a lie detection test. Despite these methods are not attacks themselves, they are an opportunity to develop new adversarial attacks against BCIs, and are defined as:

- *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.

It is important to note that the adversarial attacks detailed for this phase have only been conducted against data confidentiality. 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 on users.

Focusing on the countermeasures to mitigate these attacks, Ienca et al. [7] indicated that specific training sessions could be beneficial to protect users against potentially unsafe stimuli related to authentication methods and banking-related information. In addition, the inclusion of demos and serious games in commercial BCI devices may educate them in the risks of these technologies. However, these countermeasures

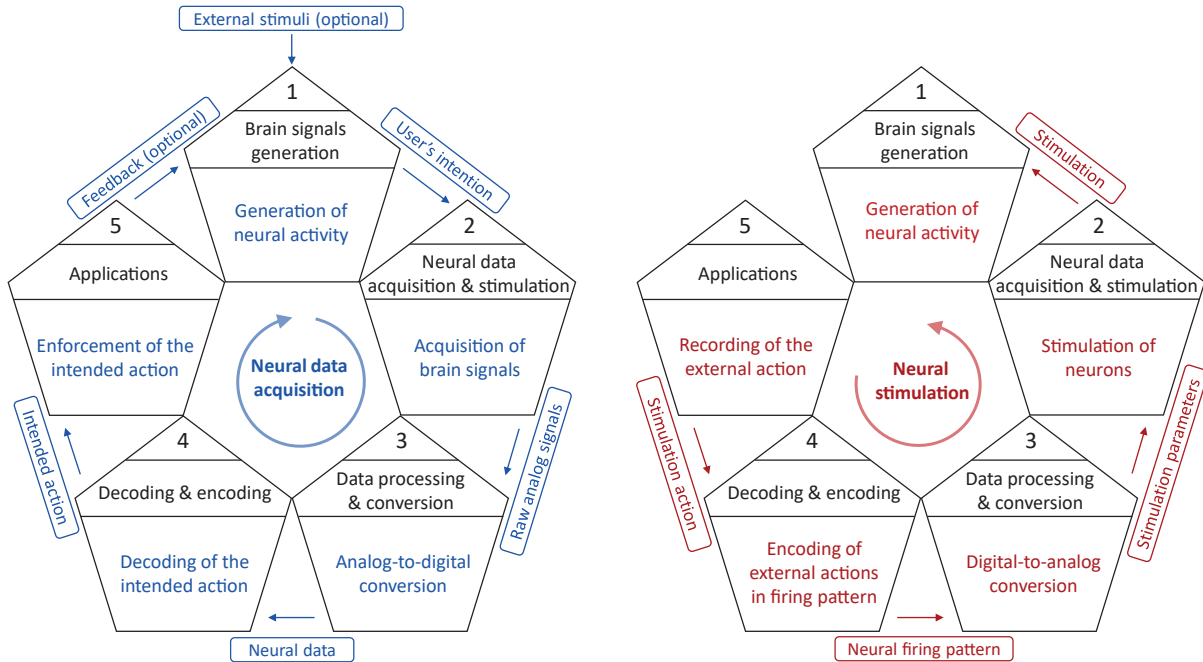


Fig. 8. Bidirectional BCI functioning cycle representing, in black, the common phases for neural data acquisition and brain stimulation. (Left side) Representation, in blue, of the processes performed and the data transferred by each phase of the neural data acquisition process. This cycle can be seen 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.

can only be applied when the user is aware of the stimuli. Because of that, we consider that adversarial attacks in this phase 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 analysing if the multimedia contents showed to users, such as images or videos, have been maliciously modified [62], [63], even if they are subliminal.

### B. Phase 2. Neural data acquisition & stimulation

This second phase is focused on the interaction with the brain to acquire brain waves or perform neural stimulation. *Replay* and *spoofing attacks* have been detected in the literature for this phase. Replay attacks consist in the retransmission of previously acquired neural data to perform a malicious action. For example, to impersonate one of the legitimate participants of the communication [64]. These attacks have been widely considered in computer networks [65] (e.g. routing protocols and authentication mechanisms). On the other hand, spoofing attacks intent to masquerade an entity of the communication, transmitting malicious data. Common spoofing attacks in network communications are, among others, IP spoofing, MAC spoofing [66] and DNS spoofing [64]. However, both attacks also are applicable to BCI, as detected by Li et al. [1] for neural data acquisition. On the other hand, *jamming attacks* transmit wireless noise signals that decrease the SNR on the receiver side and therefore disrupt the wireless communication by affecting its availability [67], [68]. Despite several types of jamming

strategies have been defined in the literature according to their functioning, this work considers only the most relevant for BCI [67]–[69]. In permanent attacks, the jamming signal is continuously transmitted, whereas reactive attacks only transmit a signal if the *jammer* detects a legitimate transmission active.

Regarding the impacts produced by the previous attacks, Li et al. [1] identified a combination of replay and spoofing attacks in which synthetic EEG signals can be crafted from historical EEG data and impersonate the legitimate brain waves, affecting their integrity. They also documented impacts on the availability, where the acquisition process was disrupted. In addition, we detect a new opportunity applying these attacks to the stimulation scenario. In this sense, attackers can disrupt the stimulation process or acquire and modify the raw stimulation pattern used by the BCI to maliciously stimulate the neurons, affecting their integrity and availability. We consider that these attacks can also derive in *hijacking attacks*, as attackers can take complete control over the device, affecting the integrity and availability of the BCI. In relation to jamming attacks, it is important to highlight that they affect both acquisition and stimulation procedures of BCI, but they generate different impacts. Taking into account neural data acquisition, an attacker would aim to prevent the electrodes to capture brain signals due to the noise transmitted, as pointed out by Ienca et al. [7]. Based on Vadlamani et al. [67], we also detect this problem in neural stimulation, where jamming attacks can override the

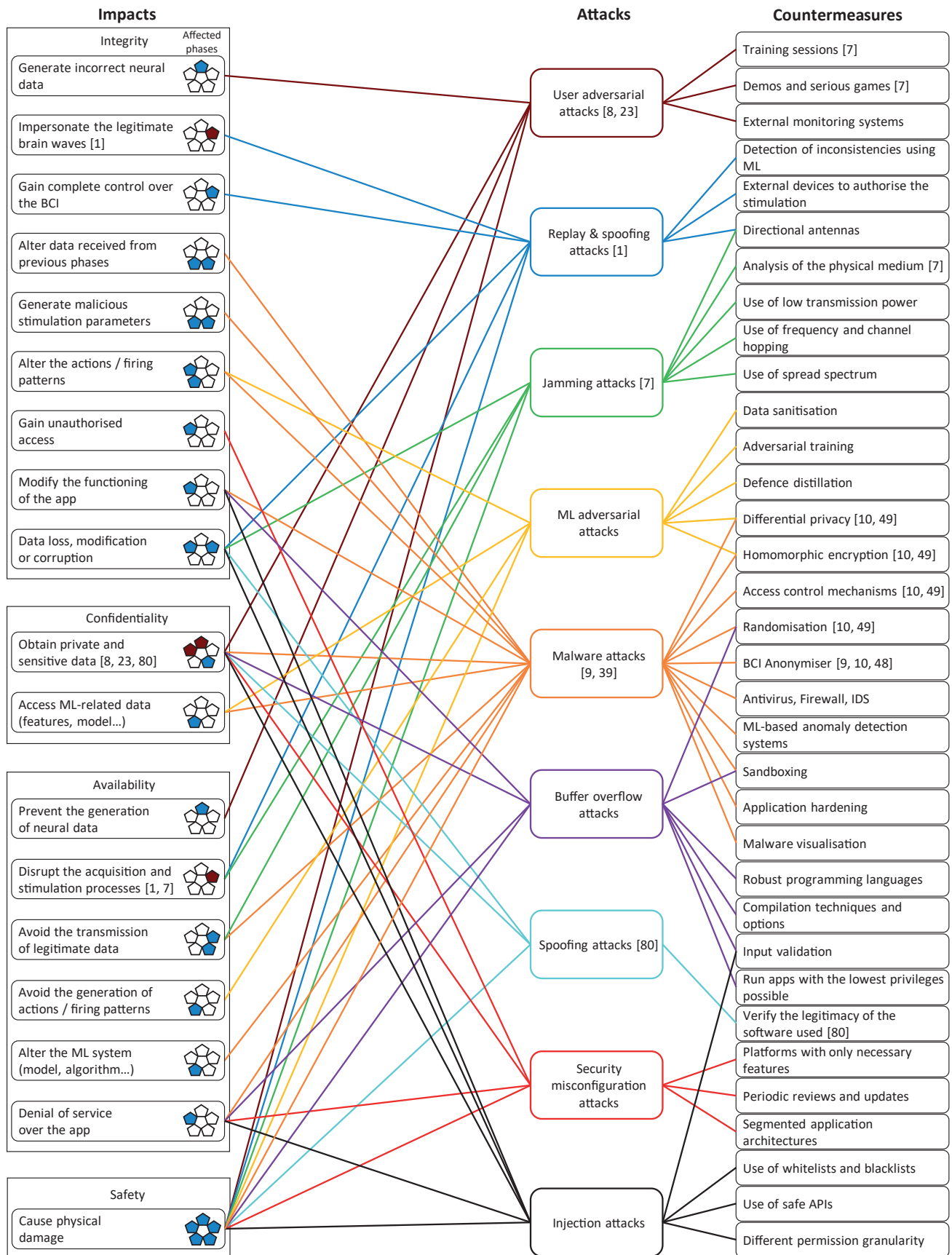


Fig. 9. Relationship between the attacks, impacts and countermeasures over the BCI cycle. The phases of the cycle coloured in red for each impact represent issues documented in the literature, while those marked in blue are our contribution. The attacks, impacts and countermeasures followed by references have been documented in the literature, and those without a cite represent our contribution.

legitimate signals emitted by the BCI electrodes if they are transmitted with enough power [67]. We identify moreover that spoofing attacks can be present in this context, where the legitimate transmission of the BCI is masqueraded, affecting information integrity and availability. Finally, the previous attacks can derive in users' physical damage, affecting their safety.

Regarding the countermeasures to detect and mitigate replay and spoofing attacks, the techniques used in computer networks are not applicable in this scenario, as they are related to specific technologies and protocols. To address these issues in BCI, we consider the use of ML in the acquisition scenario as a promising alternative to analyse the received neural information and detect inconsistencies, such as duplicated signals or representative patterns [70]. Taking into account neural stimulation, there are no global solutions to avoid a malicious attack. However, if the BCI is based on Implantable Medical Devices (IMD), external devices to authenticate and authorise the stimulation actions can be used [70]. Related to the mitigation of jamming attacks, several detection mechanisms and countermeasures have been documented [67]–[69]. In summary, all detection procedures are based on an analysis of the medium to detect abnormal behaviour, as also identified for neural data acquisition by Ienca et al. [7]. As proposed countermeasures, Vadlamani et al. [67] identified the use of low transmission power as a possible solution to harden the detection of the legitimate transmission, as well as the use of directional antennas oriented to the brain to avoid the jamming. The use of frequency hopping [69] and channel hopping [68] after a certain duration of time also aim to reduce the impact of these attacks. These hopping models are based on a pseudorandom hopping pattern previously known by sender and receiver. In addition, Spread Spectrum (SS) techniques are used to transmit the information in a wider bandwidth and thus avoid the interference. Two main SS techniques are indicated: *Frequency Hopping Spread Spectrum (FHSS)*, which uses frequency hopping, and *Direct-Sequence Spread Spectrum (DSSS)* [64], [67], [69], that utilises pseudo noise to modify the phase of the signal. Finally, we detect that the use of directional antennas is also a possible solution for replay and spoofing attacks.

### C. Phase 3. Data processing & conversion

This phase performs the data processing and conversion tasks required to allow neural data and actions to be ready for subsequent stages. Although the literature has not detected cybersecurity problems in this phase, according to the aspects indicated by Bonaci et al. in [9], [39] we identify *malware attacks* as the most damaging ones. Malware attacks focus on malicious software aiming to gain access to computational devices to perform concrete actions. There is a multitude of different types and families of malware with different objectives, propagation vectors and infection methods [71],

[72]. Considering their propagation mechanisms, worms spread themselves over the network exploiting concrete vulnerabilities, activated without explicit user interaction [65]. In contrast, viruses typically require user interaction to infect the device. Both worms and viruses can contain a payload which defines a malicious action to perform on the device, such as corruption of information or services. Focusing on BCIs, malware attacks are candidates to affect both acquisition and stimulation processes, impacting the tasks performed in this phase. Specifically, we identify that malware can disrupt the analog-to-digital conversion that takes place during neural data acquisition, as well as the translation of firing patterns to particular stimulation devices.

In this context, we identify that malware attacks have an impact in 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. Focusing on data confidentiality, these attacks can gather the sensitive data managed in this phase, both analog and digital, and send it to the attackers. For example, information about private thoughts or neurological treatments. In terms of data and service availability, both acquisition and stimulation are potentially vulnerable against malware that avoid the transmission of the data to subsequent phases of the cycle. Finally, the previous attacks on integrity and availability are also a threat against the physical safety of users, generating damaging stimulation patterns or dangerous actions finally sent to applications.

Regarding the countermeasures to mitigate the previous attacks and reduce the impacts, Chizeck et al. [48] defined a US patent application entitled “Brain-Computer Interface Anonymize” that proposes a technology capable of processing neural signals to eliminate all non-essential private information [9], [10]. As a result, sensitive information is never stored in the BCI device or transmitted outside. We identify that this method is specially relevant in this phase, as it is the first stage after the acquisition process by the BCI. 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. On the other hand, the countermeasures to mitigate malware depend on their type and behaviour. Considering the protection of individual devices, *antivirus* solutions perform both static and dynamic analysis to detect anomalies in the BCI system. For example, by the use of signatures to identify well-known families of malware, the analysis of payloads or the execution of the potential malware in isolated spaces to study its behaviour, and thus avoid the software infection. In addition, perimeter security mechanisms, such as *firewalls* and *Intrusion Detection Systems (IDS)* have been considered, responsible for

analysing all incoming and outgoing communication of the device [66], [72]. We also propose the use of ML anomaly detection systems to identify potential malware threats [70]. Finally, Chakkaravarty et al. [71] reviewed current persistent malware techniques able to bypass common countermeasures and proposed mitigation techniques, such as *sandboxing* [73], *application hardening* [74] and *malware visualisation* [75]. It is important 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 IV).

#### D. Phase 4. Decoding & encoding

*Decoding & encoding* is the phase focused on the identification of the action intended by the users in neural data acquisition, or the specification of the neural firing pattern in neurostimulation. Considering its cybersecurity problems, malware attacks have been identified in the literature by Bonaci et al. [9], [39] in a general way, and we detect that the same types of malware described in the *Processing & conversion* phase are also applicable in the current one. Specifically, they can serve as an opportunity for attackers to alter the identification of intended actions or modify the legitimate firing patterns. However, we consider that *adversarial attacks* are the biggest concern in this phase, when ML techniques are used. These attacks have been introduced for the *Brain signals generation* phase but, in this context, they affect all types of ML models ever studied over very different data types, such as images, audio or text, as stated by Finlayson et al. [57]. Because of that, models both accurate and robust against this kind of attacks are currently an open challenge. Liu et al. [58] identified security threats against both ML training and testing phases. On the one hand, two learning approaches exist in the training phase: supervised and unsupervised. Supervised learning is vulnerable to *poisoning attacks*, where attackers introduce adversarial samples with incorrect labels to the data set, aiming to change the training data distribution. These problems are also extensible to model retraining. In addition, clustering approaches used in unsupervised training are also sensitive to adversarial attacks. On the other hand, attacks on the testing phase focus on exploiting vulnerabilities of trained models, by the use of crafted samples, where several specific attacks have been documented. *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 [76]. In *white-box attacks*, adversaries have knowledge about the model, while in *black-box attacks*, they only have access to the model through a limited interface.

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, as well as overriding

the output of the current one. That is, disrupt the action sent to applications in the acquisition process, or the firing pattern in neural stimulation. In addition, malware affects the availability of the ML process by the alteration of the trained model or the ML algorithm. Considering data confidentiality issues, 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 physical integrity of users. 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. Taking into account data confidentiality, Shokri et al. [77] demonstrated that ML models are sensitive against adversarial attacks, aiming to detect if a sample was in the model's training data set. Finally, the use of malicious samples, as is the case of poisoning attacks, alter the ML system, deriving in physical harm.

To mitigate the attacks on the ML training phase affecting integrity and availability, we have identified several techniques proposed in the state of the art for generic adversarial attacks, that can serve as an opportunity to improve the security of BCI. *Data sanitisation* consists of the rejection of samples that will produce a negative impact on the model, preprocessing and validating all input containing adversarial information. However, this initiative highly depends on the domain and application environment. Jagielski et al. [78] proposed a similar approach against poisoning attacks applied to regression techniques, where noise and *outliers* are suppressed from the training data set. Nevertheless, it does not prevent attackers from crafting samples similar to those generated by the legitimate distribution. *Adversarial training* aims to include adversarial samples in the training process to allow the recognition of attacks in the future. *Defence distillation* focuses on the creation of a second model based on the original, with less sensitivity regarding input perturbations and offering smoother and more general results [58], [76]. However, adversarial training and defence distillation 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 optimisation. Goodfellow et al. [76] 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. [58] documented the integration of different techniques to mitigate the attacks, called *ensemble method*. In addition, they indicated two methods that can be applied in both training and testing phases. *Differential privacy* applies randomisation techniques over the training phase to preserve the privacy of the information and then prevent its leakage against attacks. *Homomorphic encryption* offer encrypted information to the ML system to protect the privacy of the information used as



input [10], [58], [79].

#### E. Phase 5. Applications

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 a robotic limb. From the perspective of neural stimulation, applications are the entry point of the information to be transmitted to the brain, like sensory stimuli in prosthesis or cognitive enhancement. In this section we consider attacks on applications, without analysing their communication with external systems, which are addressed in Section IV-A. 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 [80]. *Malware attacks* have also been identified as a threat in BCI [1], [9], [39]. In this sense, the families of malware applicable to this phase are the same as detailed in Sections III-C and III-D. In addition, we have found several opportunities related to cyberattacks performed against applications. *Security misconfiguration* is a type of security weakness that can exist at any level of the application stack, affecting network services, servers, platforms, databases, frameworks, virtual machines, containers or storage [81]. These weaknesses are exploited by a wide variety of security attacks. However, the detailed analysis of these concrete attacks is out of the scope of this work, and only general aspects related to security misconfiguration attacks are addressed. *Buffer Overflow (BO)* attacks occur when it is possible to access out-of-bounds memory spaces due to insecure software implementations [82]. Concretely, they take advantage of software operations over memory buffers, whose boundaries are not well managed, allowing attackers to read from or write to memory locations placed before the beginning or after the end of the buffer [83]. This also derives in the execution of malicious code, the access to restricted information or even to crash the system [82], [84]. A well-known example of BO is the vulnerability detected in the implementation of TLS and DTLS in OpenSSL, where the code uses a number from the input without proper verification, allowing an attacker to read private keys [85]. Finally, *injection attacks* occur when the input presented to an interpreter contains special elements that can modify how it is parsed. That is, hostile data used as an injection vector, such as environment variables or parameters, taking advantage on a lack of verification of the input and therefore disrupting the separation between the control plane and the data plane. These vulnerabilities are often found in a large variety of services, like SQL, NoSQL, LDAP and XPath queries, format string issues an even OS commands [86], [87].

Considering the impact of the previous attacks, although applications created by *spoofing attacks* mainly affect data integrity, they also have an impact on data confidentiality, as they can present malicious stimuli to obtain sensitive

neural information, such as specific thoughts or beliefs [80]. *Malware attacks* affect the applications integrity by the alteration of their services and capabilities, such as disable the encryption of information. In addition, they can compromise applications confidentiality, gaining access to sensitive information such as medical records and user profiles used during neurostimulation treatments. With regard to the availability of the application, malware attacks can derive in denial of service over the application, having impact in processes such as controlling prosthetic limbs or wheelchairs. In the context of *misconfiguration attacks*, we consider that data integrity issues can arise, where attackers can take advantage of the system to gain unauthorised access. For example, by exploiting weak access permissions or the lack of input validation on frameworks used to develop BCI applications. Data confidentiality issues are also present, for example, on configuration files that have static predefined passwords in them, allowing attackers to gain access to users' private data. In addition, they can be a consequence of integrity attacks, as they can derive in leakage of sensitive information. Applications availability problems are also possible, as a misconfiguration issue can serve as a first step to disrupt the normal behaviour of the application. Several misconfiguration problems have been identified by the Common Weakness Enumeration (CWE) [88], which is a community project owned by the MITRE Corporation [89] that aims to offer an extensive compilation of software weakness types. *BO attacks* can derive in the execution of unauthorised code or commands, where an attacker can alter the normal functioning of the application or access to sensitive information [90]. In addition, 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. Moreover, service availability can be affected by attacks aiming to crash or exit applications, or by the increase of CPU and memory consumption [91]. Related to the impact of *injection attacks*, they can aim to execute unauthorised code or commands, affecting the integrity, confidentiality and availability of the BCI [92], [93]. Focusing on integrity, they can produce data loss, modification and corruption, affecting the stability of applications [86], [87]. In terms of confidentiality, they can produce the disclosure of sensitive information to unauthorised parties [86], [87], such as insurance companies aiming to select the best candidates for their products [80]. Availability can be affected by a denial of access over an authentication system, disrupting vital processes such as clinical neurostimulation [86]. In addition, injection attacks against the OS can also affect applications, as they allow attackers to gain access over the system and therefore affect the integrity and confidentiality of files, directories and application data, as well as disrupt the availability of the system, producing crash, exit or restart actions [93]. Moreover, it is important to highlight the impact of injection attacks over widely extended database systems, such as SQL or LDAP, that can produce a high degradation

of applications in terms of integrity, confidentiality and availability [94]. In relation to safety, all these attacks can force applications to send malicious stimuli or actions that derive in physical harm [80]. Finally, most APIs to develop applications offer full access over the information and do not offer any limitations on the stimuli presented to users, which generates confidentiality issues [1], [8]–[11], [23].

To mitigate *spoofing attacks*, it is necessary to verify the legitimacy of the applications, and ensure a sufficient control on the app stores [80]. When it comes to *malware attacks*, the same countermeasures proposed for the *Data processing & conversion* phase are also applied for applications. That is, the use of antivirus, firewall, IDS and anomaly detection systems to detect and mitigate the attacks. In addition, Takabi et al. [10], [49] proposed the use of access control mechanisms over the information to restrict its access and thus mitigate confidentiality attacks. They also indicated the use of randomisation and differential privacy. In addition, 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. We identify as an opportunity for BCI some preventive actions against *misconfiguration attacks* defined by the Open Web Application Security Project (OWASP) [81], such as the use of minimal platforms with only necessary features, components, libraries and software to reduce the probability of misconfiguration issues. In addition, a periodic review and update of configuration parameters are also positive as part of the management process of applications. Moreover, it is necessary to create segmented application architectures that offer a division between components and defines different security groups, by the use of Access Control Lists (ACLs). In relation to *BO*, in the software requirement phase, it is important to define a language that protects against BO, such as Java or Perl, as in C/C++ the developer has direct access to memory and it is prone to attacks. In addition, some compilers provide mechanisms that mitigate BO, despite they can only detect certain types, as well as address sanitation to detect out-of-bounds accesses. They also usually offer features to randomly arrange the position of the program and libraries in memory, which difficult the attacks. However, these compiler techniques are typically not implemented by default to improve the efficiency [82]. In the implementation phase, 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 run using the lowest privileges possible and even isolated using sandbox techniques [90], [91], [95]. To detect *injection attacks*, both static and dynamic analysis of applications source code have been proposed, in addition to the automated testing of parameters, headers, URLs, cookies and data inputs [86]. Considering countermeasures for these attacks, it is necessary to escape all special characters included in the input to avoid attacks as SQL injection [86], [93]. Furthermore, this validation can be extended, assuming that

all input can be malicious and, because of that, the use of whitelists and blacklists have been proposed, rejecting any input that does not conform to the requirements specified, or transforming them into valid inputs. To perform this validation, all relevant properties must be considered, such as length, type of input or syntax [92]. In addition, the use of safe languages and APIs that include these mechanisms releases developers to perform these validations manually and reduces the probability of errors [86], [87]. Focusing on attacks on the OS, the CWE identifies several solutions. First, the use of sandbox techniques to define strict boundaries between processes and the OS [93]. In addition, the definition of different permissions on the system and thus prevent access over privileged files [92]. Moreover, error messages must contain minimal but descriptive details, ensuring that there is no leakage of sensitive information.

#### IV. CYBERSECURITY 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 in two main families, which are characterised by the BCI cycle implementation and its application scenario. In contrast to Section III, where the cybersecurity analysis is independent of the deployment, this section reviews the state of the art of existing cyberattacks affecting the devices implementing each phase of the BCI cycle, as well as their impacts and countermeasures. New opportunities, in terms of cyberattacks and countermeasures, missed by the literature are also highlighted in this section. Fig. 10 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.

##### A. Local BCI

Local BCI deployments are characterised by managing the neural acquisition and stimulation processes of single users. This architecture typically deploys the BCI phases between two physical devices, as represented in Fig. 10. The first one, identified as *BCI device*, focuses on neural acquisition and stimulation procedures (phase 1 of the BCI cycle), whereas BCI applications (phase 5) are executed by a Near Control Device (NCD), which is a PC or smartphone that controls the BCI device using either a wired or wireless communication link. The phases 3 and 4 of the cycle can be implemented equally in both devices, being the final decision made by manufacturers. At this point, it is important to note that alternative designs can arise due to specific requirements of the deployments, such as the presence of multiple users.

This kind of architectural deployment is the most commonly implemented for consumer-grade BCI, where commercial brands like NeuroSky or Emotiv focus on scenarios such

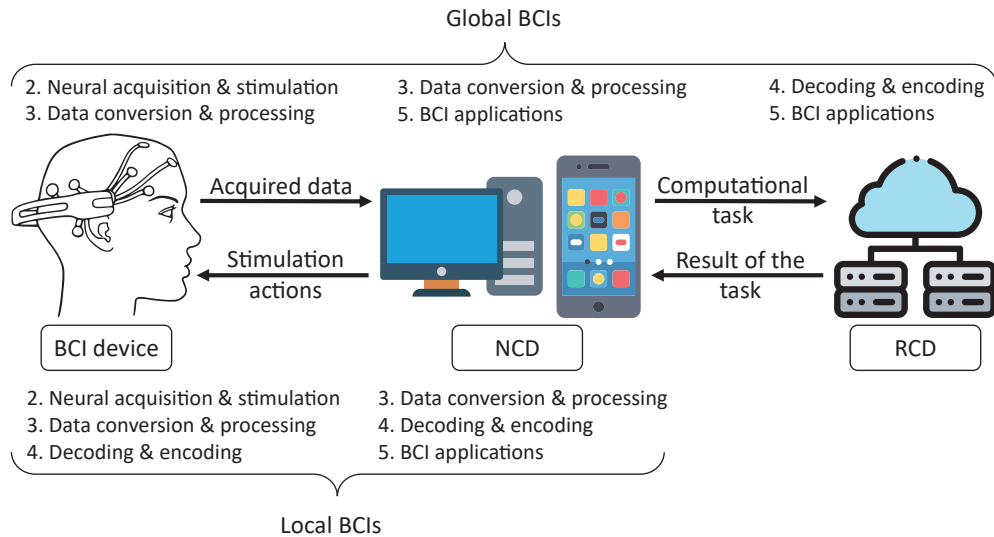


Fig. 10. Representation of Local BCI and Global BCI deployments, indicating the communication between their elements and the stages of the BCI cycle that each element implements according to the architectural deployment.

as gaming and entertainment [8], [25], [27]. Neuromedical scenarios also use this approach, where the acquisition and stimulation processes are managed by an NCD placed in the clinical environment. 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.

From the cyberattacks perspective and focusing on BCI devices, Ballarin et al. [80] identified attacks affecting the device *firmware* through a configuration link (e.g. USB ports), having an impact on data integrity and confidentiality, also generating disruptions on the system. Moreover, we identify that they can serve as an opportunity for attackers to generate safety problems. Ienca et al. [6], [7] documented *cryptographic attacks*, indicating that the 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. In addition, we identify that they produce service availability and safety issues if they are able to modify the data. Besides, Camara et al. [70] highlighted that attackers can focus on draining the battery of IMDs and thus affect both service availability and users physical safety. Considering NCDs, Ballarin et al. [80] identified *social engineering and phishing attacks* 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 [96] and those based on botnets [65], [66], [97], 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 [98], affecting service and data integrity, confidentiality and availability. Focusing on the communication between BCI devices and NCDs, Sundararajan et al. [11] 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 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. Further integrity impacts have been documented in the literature, where attackers can intercept and modify sensitive data even when encryption is used [1], [11], [49], [80]. These attacks are related with the *cryptographic attacks* described above, where a 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 will have a higher impact if the system is used by multiple users.

With the goal of mitigating some of the previous cyberattacks, different countermeasures have been proposed. Related to *firmware attacks*, Ballarin et al. [80] proposed the encryption of the firmware, as well as an authenticity verification through hash or signature. Camara et al. [70] proposed the use of access control mechanisms placed in external devices, anomaly detection systems and user

notification mechanisms to face battery drain attacks. In addition, the use of strong cryptographic mechanisms and the latest protocol versions is determinant to avoid *cryptographic attacks*, *man-in-the-middle attacks* and *sniffing attacks* [11], [80]. In addition, the anonymisation of the information transmitted by the BCI to the NCD has also been recommended against attacks that have an impact on confidentiality; for example, by the use of the BCI Anonymiser [9], [39], [49]. *Social engineering and phishing attacks* focused on credential theft can be reduced implementing a double authentication factor to access the BCI and proper access control mechanisms [10], [80]. General malware threats having impacts on NCDs can be evaded applying the malware countermeasures indicated in Section III-C, 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. [99] for Medical Cyber-Physical Systems (MCPS), can also be used in this context to detect, classify and mitigate ransomware attacks. With regard to 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 certain communication flows [?], [100], [101]. Finally, we consider that the recommendations of the U.S. Food and Drug Administration (FDA) for premarket and postmarket management of cybersecurity in medical devices should be considered in the context of BCI [102]–[104].

## B. Global BCI

Global BCI architectures are focused on the management of neural acquisition and 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 Fig. 10. In this family, the BCI device remains focused on neural 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), which represents 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 IV-A 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 be applied to RCDs. However, these later attacks are addressed in a general way, as specific cloud computing attacks are outside the scope of this article.

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 is stored and managed in a common infrastructure. Several application scenarios have been detected in the literature using this architecture, whose temporal evolution is addressed in more detail in Section V. On the one hand, Zhang et al. [105] defined the concept of the Internet of Brain, also known as BtI, where the BCI uses an NCD to access Internet services, such as search results or social media. Lebedev et al. [18] also described experiments where monkeys controlled remote robotic arms using BCI devices. In addition, Martins et al. [106] documented a fusion between neuralnanorobotics and cloud services to acquire knowledge, defining the concept of Human Brain/Cloud Interface (B/CI). On the other hand, BtB allows multiple individuals to exchange neural information, using both neural recording and stimulation procedures [18]. Pais-Vieira et al. [13] documented the real-time exchange of information between the brain of two rats. Rao et al. [107] deployed this architecture in the context of BtB communication applied to video games, where a participant imagined hand movements that were transmitted over the Internet to a second participant neurally stimulated to press the control to shoot. Jiang et al. [16] evolved this idea, developing a collaborative communication between brains to perform movements in a Tetris-like game. A specific type of BtB communication is a Brainet, based on a network of multiple interconnected brains to achieve a common goal, as defined by Pais-Vieira et al. [15], who established a neural communication between multiple rats. They can be used to transmit neural information between the participants, allowing distributed and parallel computing architectures. Ramakrishnan et al. [108] used the concept of Brainets in monkeys, where they collaborated to move an avatar arm with their neural activity. At this point, it is important to highlight that a Brainet can also be implemented in a Local BCI architecture, without an Internet connection. From the commercial point of view, Emotiv allows users to contrast their data with the data stored by other users, as well as keep user neural recordings in the cloud to visualise and manipulate them, also offering an API called Emotiv Cortex [109].

Considering the attacks on this deployment, the issues documented in Section IV-A 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. In addition, Takabi et al. [10] detected that BCI applications can 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. [80] identified that *man-in-the-middle attacks* can occur in the

communication channel between NCD and RCD, affecting the integrity, confidentiality of the data transmitted and the service availability. They also detected that attacks on RCDs can 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. On the other hand, we identify that this architecture is quite similar to those defined and implemented for IoT scenarios, where constrained devices communicate with external services via intermediate systems, especially in the case of Brainets, where multiple devices interact between them. Because of that, we detect that most of the cybersecurity attacks and impacts defined by Stelliós et al. [110] 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 [111]. This relationship between IoT and external services has been previously studied in the context of cloud computing [112]. Despite the advantages, attacks on cloud computing can impact integrity, confidentiality and availability in different levels of the cloud architecture, such as infrastructure, networking, storage and software [113], [114]. 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 [115]. 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 [116]–[118]. Malware attacks are also present in cloud environments, where ransomware and botnets are common threats [114]. Focusing on general cloud computing countermeasures, Amara et al. [119] identified security threats and attacks, as well as the mitigation techniques against them. The use of honeypots, firewalls and IDS in cloud scenarios can be used to reduce the impact of malware attacks [117].

Fig. 11 summarises 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, organised by category. For each impact, we indicate the specific attacks that cause the impact, and which elements of the architectural deployments presented in Fig. 10 are affected. In addition, the issues on the communication links between these elements are considered. Specifically, the attacks and elements identified in red represent issues detected in the literature, whereas those in blue are our contribution. Finally, this figure lists countermeasures detected both in the literature and by us, associating each attack with a list of countermeasures. The colour and reference criteria used before for the impacts also applies for the countermeasures, where an attack represented with a particular colour indicates that all their countermeasures have the same colour.

One of the first BCI solutions was developed at the end of the 1990s. It supposed a major advance in the medical industry, specifically in neurorehabilitation, bringing to the reality the mental control of prosthetic limbs and wheelchairs [120]. During the decade of the 2000s, a new generation of neuroprosthetic devices was designed to restore the mobility of patients severely paralysed, creating communication links between the brain and a wide variety of actuators, such as robotic exoskeletons [18]. This trend in the BCI field derived in new paradigms and scenarios in the decade of the 2010s, where BCIs interact with external networks and services defining the concept of BtI [50], [105]. In addition, bidirectional BCIs were defined, where acquisition and stimulation procedures are used together to acquire brain activity and deliver feedback to the brain or peripheral nerves. This allowed the creation of direct communications between two brains, known as BtB [13], [14]. 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 [15], [16]. Fig. 12 illustrates this evolution of the literature, indicating the years of publication and approaches.

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) [121]. Canada, has launched its own research line, called the Canadian Brain Research Strategy [122], [123]. On the other side of the Atlantic ocean, the European Union has also supported different projects, such as the Human Brain Project (HBP) [124] or the Brain/Neural Computer Interaction (BNCI) project [125], [126]. Asia has also promoted several initiatives such as the China Brain Project [127] or the Brain/MINDS project in Japan [128]. All the previous initiatives and projects aim to advance the understanding of the human brain by the use of innovative technologies. As a consequence, emerging technologies offer precise acquisition and stimulation capabilities that enable novel 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 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 towards 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 summarised the evolution of BCI and its trend, below we highlight the most important current and future

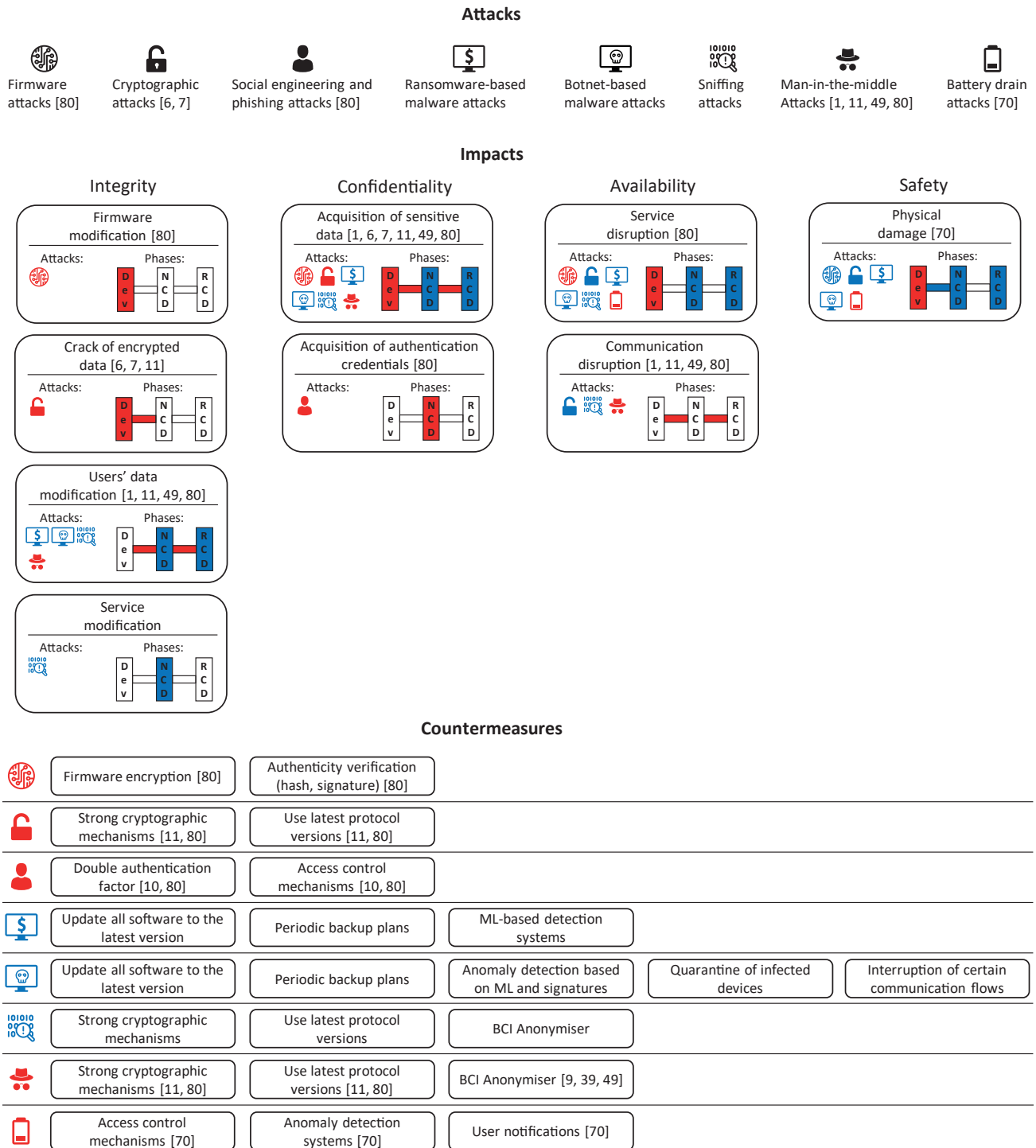


Fig. 11. List of attacks, impacts and countermeasures associated with the BCI architectural deployments. Attacks and elements of the deployments indicated in red represent information detected in the literature, while the blue colour represents our contribution.

challenges concerning cybersecurity on BCI.

### A. 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 [12]. Moreover, deployments integrating the communication between several BCIs are ad-hoc; that is, they are designed and implemented considering only the requirements of a particular scenario. In this context, the current trend of BCI towards paradigms such as the IoT and cloud computing will require an improvement of their interoperability, as it is essential to ensure the future expansion of BCI technologies. In addition, the lack of interoperability limits the definition of general 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 standardised APIs, communication technologies and protocols to offer seamless protection on BCI. Based on the previous limitations, we propose the use of ontologies to represent neural information in a formal and standardised fashion. Because of that, different companies and products would use a common representation to ease the data interpretation, processing and sharing. This homogenisation would have a positive impact on cybersecurity, enabling the design and deployment of new protocols and mechanism enabling the secure exchange of particular pieces of sensitive data between independent BCI solutions.

### B. Extensibility of BCI designs

Extensibility refers to the ability of BCIs to add new functionality and application scenarios in a dynamic way. Nowadays, BCI devices suffer a lack of extensibility, as they are manufactured 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 [11]. Since each application scenario has its own requirements and restrictions, the trend towards Global BCI will need new automatic and flexible architectures and processing mechanisms over the acquired neural data. These aspects also affect the cybersecurity 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. Because of that, and in conjunction with a lack of interoperability, the cybersecurity 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

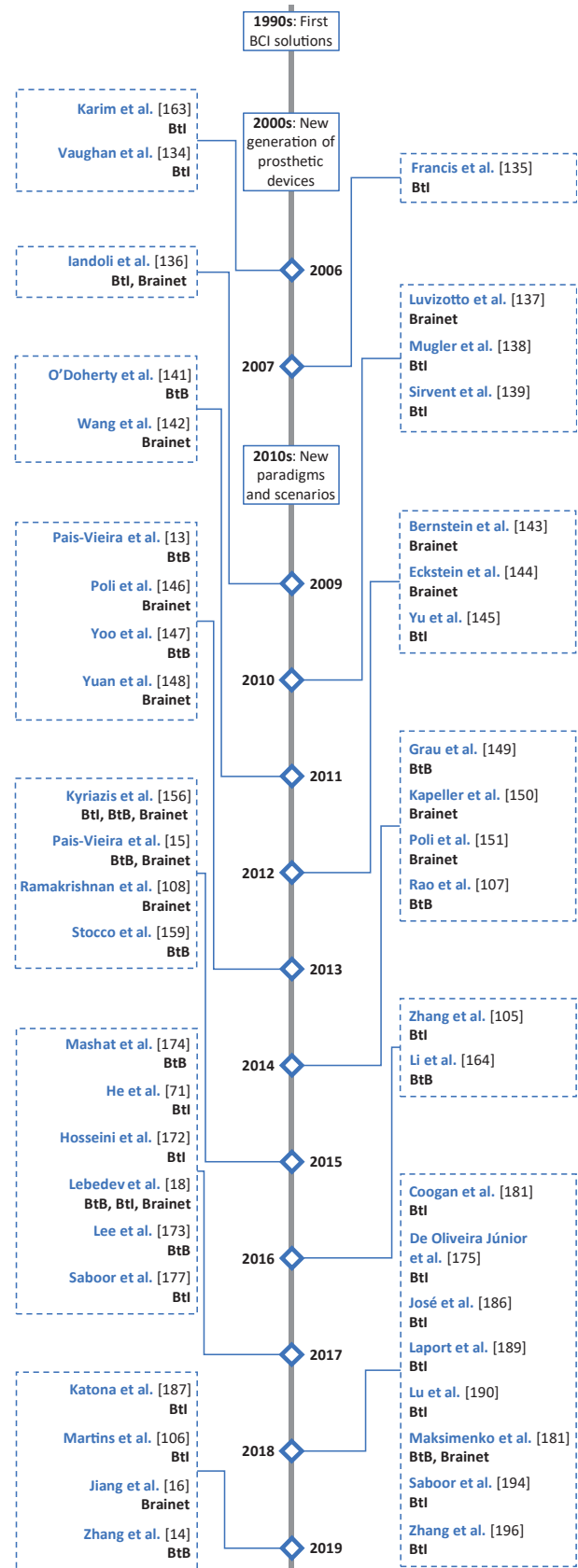


Fig. 12. Timeline of the evolution of BCI research, seen from the perspective of BtI, BtB and Brainet approaches.

software, instead of hardware, allowing developers to change the behaviour of the system. Another possible solution is a modular design of BCI, including supplementary modules according to the requirements.

### C. Data protection

Current BCI architectures and deployments do not consider the protection of neural data and personal information, as detected in the literature [12], [49], [50]. 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 authorisation. The evolution of BCI towards 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 in a secure way. To improve this situation, we propose the development of policy-based solutions that allow users to define their privacy preferences based on their particular context. In addition, we propose the use of user-friendly systems that also help users proposing privacy-preserving recommendations. These initiatives must be also aligned with the data protection law applicable in each country.

### D. Physical and architectural BCI threats

Nowadays, BCI designs and deployments do not consider cybersecurity issues such as the protection of communications, processing, storage and applications. In addition, the lack of BCI standards and, specifically, cybersecurity standards, prevent the homogenisation of the implemented solutions [9]–[12]. The expansion of BCI solutions will require robust dynamic cybersecurity mechanisms to face future challenges. Moreover, the development of more precise BCI devices, together with the integration of a large number of devices and systems, will derive in massive production of sensitive data. In our opinion, this context will 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 the use of 5G network technologies, since they have been designed to support a great number of devices, necessary for BtB and Brainet scenarios. Specifically, we identify that techniques and paradigms associated with 5G such as Network Function Virtualisation (NFV) and Software-Defined Networking (SDN) for the virtualisation and dynamic management of network communications are useful for the development of reactive cybersecurity solutions. In addition, 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 the use of protocols such as TLS [129] or IPsec [130] as an opportunity, which offers robust mechanisms against cyberattacks. On the other hand, we detect that the application of cybersecurity standards such as the ISO 27000 [131] and the NIST Cybersecurity Framework [132] will benefit the creation of homogeneous solutions. Finally, the exchange of information between medical systems can be accomplished using well-known standards, as is the case of the HL7 standard [133].

## VI. CONCLUSION

This article performs a global and comprehensive analysis of the state of the art of BCIs in terms of cybersecurity and safety. Particularly, we have evaluated the risks, attacks, impacts and countermeasures that BCI solutions suffer from the classification, software architectural design, and implementation perspectives. Initially, we have performed an analysis of the cybersecurity risks and concerns of the most well-known BCI classifications, where we have seen that, although some risks have been identified in the literature, most of the contributions are our own. This analysis of the classifications has been useful to detect which BCI families are more sensitive, and where future cybersecurity works can focus. After that, we proposed a unified version of the BCI cycle to include neural acquisition and stimulation processes. Once having a homogeneous BCI cycle design, we identified cybersecurity 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 analysed to highlight the cybersecurity attacks and countermeasures related to each approach and thus understand the cybersecurity 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 towards interconnected devices is generating tremendous cybersecurity concerns and challenges, which will increase in the near future.

Among the learned lessons, we highlight the following nine: (1) reactive BCIs are especially sensitive against malicious external stimuli; (2) the technology used for developing BCI solutions have a high impact on cybersecurity; (3) the greater is the invasiveness of BCIs, the greater are their risks in terms of users safety and data availability and confidentiality; (4) there are no previous works in the literature that define a unified version of the BCI cycle for neural stimulation or bidirectional BCIs; (5) there is a lack of comprehensive proposals to analyse the cybersecurity issues of BCIs from a wide perspective, since the number of attacks and countermeasures described in the literature is very reduced; (6) user adversarial attacks are the most commonly studied attacks against neural data acquisition; (7) attacks against BCIs devices have been widely documented; (8) NCD devices are specially sensitive, as they are the direct



point of communication with BCIs; (9) no publications have reviewed the impacts that attacks against RCDs have on BCI deployments.

As future work, we plan to focus our efforts on the design and implementation of solutions able to detect and mitigate in real time cyberattacks affecting the stimulation process. In this context, we are considering the use of artificial intelligence techniques to detect anomalies in the firing patterns and neural activity controlled by BCI solutions in charge of stimulating the brain. In addition, 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 cyberattacks documented in this work.

#### ACKNOWLEDGEMENT

This work has been supported by the Irish Research Council, under the government of Ireland post-doc fellowship (grant GOIPD/2018/466). We would also like to thank Mattia Zago for his advice during the development of the visual support of the work.

#### REFERENCES

- [1] Q. Li, D. Ding, and M. Conti, "Brain-Computer Interface applications: Security and privacy challenges," in *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, sep 2015, pp. 663–666, doi: 10.1109/CNS.2015.7346884.
- [2] E. Khabarova, N. Denisova, A. Dmitriev, K. Slavin, L. Verhagen Metman, E. A. Khabarova, N. P. Denisova, A. B. Dmitriev, K. V. Slavin, and L. Verhagen Metman, "Deep Brain Stimulation of the Subthalamic Nucleus in Patients with Parkinson Disease with Prior Pallidotomy or Thalamotomy," *Brain Sciences*, vol. 8, no. 4, p. 66, apr 2018, doi: 10.3390/brainsci8040066.
- [3] W. J. Tyler, J. L. Sanguinetti, M. Fini, and N. Hool, "Non-invasive neural stimulation," in *Proc.SPIE*, T. George, A. K. Dutta, and M. S. Islam, Eds., vol. 10194. International Society for Optics and Photonics, may 2017, p. 101941L, doi: 10.1117/12.2263175.
- [4] R. P. Rao, "Towards neural co-processors for the brain: combining decoding and encoding in brain-computer interfaces," *Current Opinion in Neurobiology*, vol. 55, pp. 142–151, apr 2019, doi: 10.1016/J.CONB.2019.03.008.
- [5] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: security and privacy for neural devices," *Neurosurgical Focus*, vol. 27, no. 1, p. E7, 2009, doi: 10.3171/2009.4.FOCUS0985.
- [6] M. Ienca, "Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering," *Bioethica Forum*, vol. 8, no. 2, pp. 51–53, 2015. [Online]. Available: [http://www.bioethica-forum.ch/docs/15\\_{\\_}2/05\\_{\\_}Ienca\\_{\\_}BF8\\_{\\_}2.pdf](http://www.bioethica-forum.ch/docs/15_{_}2/05_{_}Ienca_{_}BF8_{_}2.pdf)
- [7] M. Ienca and P. Haselager, "Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity," *Ethics and Information Technology*, vol. 18, no. 2, pp. 117–129, jun 2016, doi: 10.1007/s10676-016-9398-9.
- [8] I. Martinovic, D. Davies, and M. Frank, "On the feasibility of side-channel attacks with brain-computer interfaces," in *Proceedings of the 21st USENIX Security Symposium*. Bellevue, WA: USENIX, 2012, pp. 143–158.
- [9] T. Bonaci, R. Calo, and H. J. Chizeck, "App Stores for the Brain : Privacy and Security in Brain-Computer Interfaces," *IEEE Technology and Society Magazine*, vol. 34, no. 2, pp. 32–39, jun 2015, doi: 10.1109/MTS.2015.2425551.
- [10] H. Takabi, A. Bhalotiya, and M. Alohaly, "Brain computer interface (BCI) applications: Privacy threats and countermeasures," in *Proceedings - 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, IEEE CIC 2016*. IEEE, nov 2016, pp. 102–111, doi: 10.1109/CIC.2016.24.
- [11] K. Sundararajan, "Privacy and security issues in Brain Computer Interface," Master's thesis, Auckland University of Technology, 2017.
- [12] R. A. Ramadan and A. V. Vasilakos, "Brain computer interface: control signals review," *Neurocomputing*, vol. 223, pp. 26–44, feb 2017, doi: 10.1016/J.NEUCOM.2016.10.024.
- [13] M. Pais-Vieira, M. Lebedev, C. Kunicki, J. Wang, and M. A. L. Nicolelis, "A Brain-to-Brain Interface for Real-Time Sharing of Sensorimotor Information," *Scientific Reports*, vol. 3, no. 1, p. 1319, dec 2013, doi: 10.1038/srep01319.
- [14] S. Zhang, S. Yuan, L. Huang, X. Zheng, Z. Wu, K. Xu, and G. Pan, "Human Mind Control of Rat Cyborg's Continuous Locomotion with Wireless Brain-to-Brain Interface," *Scientific Reports*, vol. 9, no. 1, p. 1321, dec 2019, doi: 10.1038/s41598-018-36885-0.
- [15] M. Pais-Vieira, G. Chiuffa, M. Lebedev, A. Yadav, and M. A. L. Nicolelis, "Building an organic computing device with multiple interconnected brains," *Scientific Reports*, vol. 5, no. 1, p. 11869, dec 2015, doi: 10.1038/srep11869.
- [16] L. Jiang, A. Stocco, D. M. Losey, J. A. Abernethy, C. S. Prat, and R. P. N. Rao, "BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains," *Scientific Reports*, vol. 9, no. 1, p. 6115, dec 2019, doi: 10.1038/s41598-019-41895-7.
- [17] K. Wahlstrom, N. B. Fairweather, and H. Ashman, "Privacy and Brain-computer Interfaces: Identifying Potential Privacy Disruptions," *ACM SIGCAS Computers and Society*, vol. 46, no. 1, pp. 41–53, mar 2016, doi: 10.1145/2908216.2908223.
- [18] M. A. Lebedev and M. A. L. Nicolelis, "Brain-Machine Interfaces: From Basic Science to Neuroprostheses and Neurorehabilitation," *Physiological Reviews*, vol. 97, no. 2, pp. 767–837, apr 2017, doi: 10.1152/physrev.00027.2016.
- [19] T. O. Zander, C. Kothe, S. Jatzev, and M. Gaertner, "Enhancing Human-Computer Interaction with Input from Active and Passive Brain-Computer Interfaces," in *Brain-Computer Interfaces. Human-Computer Interaction Series.*, D. Tan and A. Nijholt, Eds. Springer, London, 2010, ch. 11, pp. 181–199, doi: 10.1007/978-1-84996-272-8\_11.
- [20] K. S. Hong and M. J. Khan, "Hybrid brain-computer interface techniques for improved classification accuracy and increased number of commands: A review," vol. 11, no. JUL, p. 35, jul 2017, doi: 10.3389/fnbot.2017.00035.
- [21] V. Gilja, P. Nuyujukian, C. A. Chestek, J. P. Cunningham, B. M. Yu, J. M. Fan, M. M. Churchland, M. T. Kaufman, J. C. Kao, S. I. Ryu, and K. V. Shenoy, "A high-performance neural prosthesis enabled by control algorithm design," *Nature Neuroscience*, vol. 15, no. 12, pp. 1752–1757, dec 2012, doi: 10.1038/nn.3265.
- [22] P. Arico, G. Borghini, G. Di Flumeri, N. Sciaraffa, and F. Babiloni, "Passive BCI beyond the lab: Current trends and future directions," vol. 39, no. 8, p. 08TR02, aug 2018, doi: 10.1088/1361-6579/aad57e.
- [23] M. Frank, T. Hwu, S. Jain, R. T. Knight, I. Martinovic, P. Mittal, D. Perito, I. Sluganovic, and D. Song, "Using EEG-Based BCI Devices to Subliminally Probe for Private Information," in *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society - WPES '17*. New York, New York, USA: ACM Press, 2017, pp. 133–136, doi: 10.1145/3139550.3139559.
- [24] M. van Gerven, J. Farquhar, R. Schaefer, R. Vlek, J. Geuze, A. Nijholt, N. Ramsey, P. Haselager, L. Vuurpijl, S. Gielen, and P. Desain, "The brain-computer interface cycle," *Journal of Neural Engineering*, vol. 6, no. 4, p. 041001, aug 2009, doi: 10.1088/1741-2560/6/4/041001.
- [25] M. Ahn, M. Lee, J. Choi, S. Jun, M. Ahn, M. Lee, J. Choi, and S. C. Jun, "A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users," *Sensors*, vol. 14, no. 8, pp. 14 601–14 633, aug 2014, doi: 10.3390/s140814601.
- [26] R. Polanía, M. A. Nitsche, and C. C. Ruff, "Studying and modifying brain function with non-invasive brain stimulation," *Nature Neuroscience*, vol. 21, no. 2, pp. 174–187, feb 2018, doi: 10.1038/s41593-017-0054-4.
- [27] M. McMahan and M. Schukat, "A low-Cost , Open-Source , BCI-VR Game Control Development Environment Prototype for Game based Neurorehabilitation," *2018 IEEE Games, Entertainment, Media Conference (GEM)*, pp. 1–9, aug 2018, doi: 10.1109/GEM.2018.8516468.
- [28] J. Gomes-Osman, A. Indahlastari, P. J. Fried, D. L. F. Cabral, J. Rice, N. R. Nissim, S. Aksu, M. E. McLaren, and A. J. Woods, "Non-invasive Brain Stimulation: Probing Intracortical Circuits and Improving Cognition in the Aging Brain," *Frontiers in Aging Neuroscience*, vol. 10, p. 177, jun 2018, doi: 10.3389/fnagi.2018.00177.

- [29] M. Bikson, A. R. Brunoni, L. E. Charvet, V. P. Clark, L. G. Cohen, Z. D. Deng, J. Dmochowski, D. J. Edwards, F. Frohlich, E. S. Kappenman, K. O. Lim, C. Loo, A. Mantovani, D. P. McMullen, L. C. Parra, M. Pearson, J. D. Richardson, J. M. Rumsey, P. Sehatpour, D. Sommers, G. Unal, E. M. Wassermann, A. J. Woods, and S. H. Lisanby, "Rigor and reproducibility in research with transcranial electrical stimulation: An NIMH-sponsored workshop," *Brain Stimulation*, vol. 11, no. 3, pp. 465–480, may 2018, doi: 10.1016/j.brs.2017.12.008.
- [30] W. Legon, P. Bansal, R. Tyshynsky, L. Ai, and J. K. Mueller, "Transcranial focused ultrasound neuromodulation of the human primary motor cortex," *Scientific Reports*, vol. 8, no. 1, p. 10007, dec 2018, doi: 10.1038/s41598-018-28320-1.
- [31] J. Kubanek, "Neuromodulation with transcranial focused ultrasound," *Neurosurgical focus*, vol. 44, no. 2, p. E14, feb 2018, doi: 10.3171/2017.11.FOCUS17621.
- [32] D. Seo, J. M. Carmena, J. M. Rabaey, E. Alon, and M. M. Maharbiz, "Neural Dust: An Ultrasonic, Low Power Solution for Chronic Brain-Machine Interfaces," jul 2013.
- [33] R. M. Neely, D. K. Piech, S. R. Santacruz, M. M. Maharbiz, and J. M. Carmena, "Recent advances in neural dust: towards a neural interface platform," *Current Opinion in Neurobiology*, vol. 50, pp. 64–71, jun 2018, doi: 10.1016/j.CONB.2017.12.010.
- [34] S. A. Wirdatmadja, M. T. Barros, Y. Koucheryavy, J. M. Jornet, and S. Balasubramaniam, "Wireless Optogenetic Nanonetworks for Brain Stimulation: Device Model and Charging Protocols," *IEEE Transactions on Nanobioscience*, vol. 16, no. 8, pp. 859–872, dec 2017, doi: 10.1109/TNB.2017.2781150.
- [35] H. Zheng, Z. Zhang, S. Jiang, B. Yan, X. Shi, Y. Xie, X. Huang, Z. Yu, H. Liu, S. Weng, A. Nurmikko, Y. Zhang, H. Peng, W. Xu, and J. Zhang, "A shape-memory and spiral light-emitting device for precise multisite stimulation of nerve bundles," *Nature Communications*, vol. 10, no. 1, p. 2790, 2019, doi: 10.1038/s41467-019-10418-3.
- [36] J. Lee, E. Mok, J. Huang, L. Cui, A.-H. Lee, V. Leung, P. Mercier, S. Shellhammer, L. Larson, P. Asbeck, R. Rao, Y.-K. Song, A. Nurmikko, and F. Laiwalla, "An Implantable Wireless Network of Distributed Microscale Sensors for Neural Applications," in *2019 9th International IEEE/EMBS Conference on Neural Engineering (NER)*. IEEE, mar 2019, pp. 871–874, doi: 10.1109/NER.2019.8717023.
- [37] W. Glannon, "Ethical issues with brain-computer interfaces," *Frontiers in Systems Neuroscience*, vol. 8, p. 136, jul 2014, doi: 10.3389/fnys.2014.00136.
- [38] S. Vaid, P. Singh, and C. Kaur, "EEG Signal Analysis for BCI Interface: A Review," in *International Conference on Advanced Computing and Communication Technologies, ACCT*, vol. 2015-April. IEEE, feb 2015, pp. 143–147, doi: 10.1109/ACCT.2015.72.
- [39] T. Bonaci, J. Herron, C. Matlack, and H. J. Chizeck, "Securing the Exocortex: A Twenty-First Century Cybernetics Challenge," *IEEE Technology and Society Magazine*, vol. 34, no. 3, pp. 44–51, sep 2015, doi: 10.1109/MTS.2015.2461152.
- [40] D. D. Chakladar and S. Chakraborty, "Feature Extraction and Classification in Brain-Computer Interfacing : Future Research Issues and Challenges," in *Natural Computing for Unsupervised Learning*. Springer, Cham, 2018, ch. 5, pp. 101–131, doi: 10.1007/978-3-319-98566-4\_5.
- [41] T. Yang, S. Hakimian, and T. H. Schwartz, "Intraoperative electro-CorticoGraphy (ECog): Indications, techniques, and utility in epilepsy surgery," *Epileptic Disorders*, vol. 16, no. 3, pp. 271–279, sep 2014, doi: 10.1684/epd.2014.0675.
- [42] A. Campbell and C. Wu, "Chronically Implanted Intracranial Electrodes: Tissue Reaction and Electrical Changes," *Micromachines*, vol. 9, no. 9, aug 2018, doi: 10.3390/mi9090430.
- [43] L. Pycroft and T. Z. Aziz, "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks," *Expert Review of Medical Devices*, vol. 15, no. 6, pp. 403–406, jun 2018, doi: 10.1080/17434440.2018.1483235.
- [44] S. Waldert, "Invasive vs. Non-Invasive Neuronal Signals for Brain-Machine Interfaces: Will One Prevail?" *Frontiers in Neuroscience*, vol. 10, p. 295, jun 2016, doi: 10.3389/fnins.2016.00295.
- [45] H. S. An, J. W. Kim, and S. W. Lee, "Design of an asynchronous brain-computer interface for control of a virtual Avatar," in *4th International Winter Conference on Brain-Computer Interface, BCI 2016*. IEEE, feb 2016, pp. 1–2, doi: 10.1109/IWW-BCI.2016.7457463.
- [46] N. Bentabet and N. E. Berrached, "Synchronous P300 based BCI to control home appliances," in *Proceedings of 2016 8th International Conference on Modelling, Identification and Control, ICMIC 2016*. IEEE, nov 2016, pp. 835–838, doi: 10.1109/ICMIC.2016.7804230.
- [47] U. Chaudhary, B. Xia, S. Silvoni, L. G. Cohen, and N. Birbaumer, "Brain-Computer Interface-Based Communication in the Completely Locked-In State," *PLOS Biology*, vol. 15, no. 1, p. e1002593, jan 2017, doi: 10.1371/journal.pbio.1002593.
- [48] H. J. Chizeck and T. Bonaci, "Brain-Computer Interface Anonymizer. US Patent Application," U.S. Patent US20140228701A1, Aug. 14, 2014.
- [49] H. Takabi, "Firewall for brain: Towards a privacy preserving ecosystem for BCI applications," in *2016 IEEE Conference on Communications and Network Security, CNS 2016*. IEEE, oct 2016, pp. 370–371, doi: 10.1109/CNS.2016.7860516.
- [50] D. Sempredoni and L. Viganò, "Privacy, Security and Trust in the Internet of Neurons," *arXiv*, jul 2018. [Online]. Available: <http://arxiv.org/abs/1807.06077>
- [51] StatCounter Global Stats, "Mobile & Tablet Android Version Market Share Worldwide." [Online]. Available: <http://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide>
- [52] NeuroSky, "NeuroSky." [Online]. Available: <http://neurosky.com/>
- [53] R. D. Gavas and G. U. Navalyal, "Fast and secure random number generation using low-cost EEG and pseudo random number generator," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*. IEEE, aug 2017, pp. 369–374, doi: 10.1109/SmartTechCon.2017.8358398.
- [54] A. Muñoz, "Cryptography with brainwaves for fun and...profit?" *RootedCON 2016*. [Online]. Available: <https://www.youtube.com/watch?v=TOFNMyPe3Fw>
- [55] K. Matsushita, M. Hirata, T. Suzuki, H. Ando, T. Yoshida, Y. Ota, F. Sato, S. Morris, H. Sugata, T. Goto, T. Yanagisawa, and T. Yoshimine, "A Fully Implantable Wireless ECoG 128-Channel Recording Device for Human Brain-Machine Interfaces: W-HERBS," *Frontiers in neuroscience*, vol. 12, p. 511, 2018, doi: 10.3389/fnins.2018.00511.
- [56] P. Sarma, P. Tripathi, M. P. Sarma, and K. K. Sarma, "Pre-processing and Feature Extraction Techniques for EEG- BCI Applications-A Review of Recent Research," *ADB- Journal of Engineering Technology*, vol. 5, pp. 2348–7305, 2016. [Online]. Available: <http://journals.dbuiversity.ac.in/ojs/index.php/AJET/article/view/218>
- [57] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287–1289, mar 2019, doi: 10.1126/science.aaw4399.
- [58] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," *IEEE Access*, vol. 6, pp. 12 103–12 117, 2018, doi: 10.1109/ACCESS.2018.2805680.
- [59] K. Sowndhararajan, M. Kim, P. Deepa, S. Park, and S. Kim, "Application of the P300 Event-Related Potential in the Diagnosis of Epilepsy Disorder: A Review," *Scientia Pharmaceutica*, vol. 86, no. 2, p. 10, mar 2018, doi: 10.3390/scipharm86020010.
- [60] "EMOTIV EPOC+." [Online]. Available: <https://www.emotiv.com/epoc/>
- [61] Emotiv, "Emotiv." [Online]. Available: <https://www.emotiv.com/>
- [62] A. W. A. Wahab, M. A. Bagiwa, M. Y. I. Idris, S. Khan, Z. Razak, and M. R. K. Ariffin, "Passive video forgery detection techniques: A survey," in *2014 10th International Conference on Information Assurance and Security*. IEEE, nov 2014, pp. 29–34, doi: 10.1109/ISIAS.2014.7064616.
- [63] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digital Investigation*, vol. 10, no. 3, pp. 226–245, oct 2013, doi: 10.1016/j.diin.2013.04.007.
- [64] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Pearson, 2011.
- [65] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Pearson, 2017.
- [66] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.
- [67] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, feb 2016, doi: 10.1016/j.ijpe.2015.11.008.
- [68] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International Journal of Ad*

- Hoc and Ubiquitous Computing*, vol. 17, no. 4, p. 197, 2014, doi: 10.1504/ijahuc.2014.066419.
- [69] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, sep 2016, doi: 10.1109/JPROC.2016.2558521.
- [70] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272–289, jun 2015, doi: 10.1016/J.JBI.2015.04.007.
- [71] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Computer Science Review*, vol. 32, pp. 1–23, may 2019, doi: 10.1016/J.COSREV.2019.01.002.
- [72] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Software Quality Journal*, vol. 26, no. 3, pp. 891–919, sep 2018, doi: 10.1007/s11219-017-9368-4.
- [73] N. Miramirkhani, M. P. Appini, N. Nikiforakis, and M. Polychronakis, "Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, may 2017, pp. 1009–1024, doi: 10.1109/SP.2017.42.
- [74] V. Hauptert, D. Maier, N. Schneider, J. Kirsch, and T. Müller, *Honey, I Shrank Your App Security: The State of Android App Hardening*. Springer, Cham, jun 2018, doi: 10.1007/978-3-319-93411-2\_4.
- [75] J. Fu, J. Xue, Y. Wang, Z. Liu, and C. Shan, "Malware Visualization for Fine-Grained Classification," *IEEE Access*, vol. 6, pp. 14 510–14 523, 2018, doi: 10.1109/ACCESS.2018.2805301.
- [76] I. Goodfellow, P. McDaniel, and N. Papernot, "Making machine learning robust against adversarial inputs," *Communications of the ACM*, vol. 61, no. 7, pp. 56–66, jun 2018, doi: 10.1145/3134599.
- [77] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership Inference Attacks Against Machine Learning Models," in *Proceedings - IEEE Symposium on Security and Privacy*. IEEE, may 2017, pp. 3–18, doi: 10.1109/SP.2017.41.
- [78] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning," in *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2018-May. IEEE, may 2018, pp. 19–35, doi: 10.1109/SP.2018.00057.
- [79] A. Huertas Celdrán, G. Dólera Tormo, F. Gómez Mármol, M. Gil Pérez, and G. Martínez Pérez, "Resolving privacy-preserving relationships over outsourced encrypted data storages," *International Journal of Information Security*, vol. 15, no. 2, pp. 195–209, apr 2016, doi: 10.1007/s10207-015-0283-z.
- [80] P. Ballarín Usieto and J. Mínguez, "Avoiding brain hacking - Challenges of cybersecurity and privacy in Brain Computer Interfaces," 2018. [Online]. Available: <https://www.bitbrain.com/blog/cybersecurity-brain-computer-interface>
- [81] Open Web Application Security Project, "Top 10-2017 A6-Security Misconfiguration - OWASP," 2017. [Online]. Available: [https://www.owasp.org/index.php/Top\\_{ }10-2017\\_{ }A6-Security\\_{ }Misconfiguration](https://www.owasp.org/index.php/Top_{ }10-2017_{ }A6-Security_{ }Misconfiguration)
- [82] T. Saito, R. Watanabe, S. Kondo, S. Sugawara, and M. Yokoyama, "A Survey of Prevention/Mitigation against Memory Corruption Attacks," in *2016 19th International Conference on Network-Based Information Systems (NBIS)*. IEEE, sep 2016, pp. 500–505, doi: 10.1109/NBiS.2016.11.
- [83] P. E. Black and I. Bojanova, "Defeating Buffer Overflow: A Trivial but Dangerous Bug," *IT Professional*, vol. 18, no. 6, pp. 58–61, nov 2016, doi: 10.1109/MITP.2016.117.
- [84] MITRE, "CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer." [Online]. Available: <https://cwe.mitre.org/data/definitions/119.html>
- [85] MITRE, "CVE-2014-0160." [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>
- [86] O. W. A. S. Project, "Top 10-2017 A1-Injection - OWASP," 2017. [Online]. Available: [https://www.owasp.org/index.php/Top\\_{ }10-2017\\_{ }A1-Injection](https://www.owasp.org/index.php/Top_{ }10-2017_{ }A1-Injection)
- [87] MITRE, "CWE - CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/74.html>
- [88] MITRE, "CWE List Version 3.2," Tech. Rep., 2019. [Online]. Available: [https://cwe.mitre.org/data/published/cwe\\_{ }v3.2.pdf](https://cwe.mitre.org/data/published/cwe_{ }v3.2.pdf)
- [89] MITRE, "The MITRE Corporation," 2019. [Online]. Available: <https://www.mitre.org/>
- [90] MITRE, "CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/120.html>
- [91] MITRE, "CWE-121: Stack-based Buffer Overflow (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/121.html>
- [92] MITRE, "CWE - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/77.html>
- [93] MITRE, "CWE - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/78.html>
- [94] MITRE, "CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/89.html>
- [95] MITRE, "CWE-122: Heap-based Buffer Overflow (3.2)." [Online]. Available: <https://cwe.mitre.org/data/definitions/122.html>
- [96] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Computers & Security*, vol. 74, pp. 144–166, may 2018, doi: 10.1016/J.COSE.2018.01.001.
- [97] C. Koliás, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.
- [98] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," in *2017 International Conference on Intelligent Computing and Control (IC2C)*. IEEE, jun 2017, pp. 1–5, doi: 10.1109/IC2C.2017.8321914.
- [99] L. Fernández Maimó, A. Huertas Celdrán, Á. Perales Gómez, F. García Clemente, J. Weimer, I. Lee, L. Fernández Maimó, A. Huertas Celdrán, Á. L. Perales Gómez, F. J. García Clemente, J. Weimer, and I. Lee, "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," *Sensors*, vol. 19, no. 5, p. 1114, mar 2019, doi: 10.3390/s19051114.
- [100] P. Amini, M. A. Araghizadeh, and R. Azmi, "A survey on Botnet: Classification, detection and defense," in *2015 International Electronics Symposium (IES)*. IEEE, sep 2015, pp. 233–238, doi: 10.1109/ELECSYM.2015.7380847.
- [101] M. Mahmoud, M. Nir, and A. Matrawy, "A Survey on Botnet Architectures, Detection and Defences," *International Journal of Network Security*, vol. 17, no. 3, pp. 272–289, may 2015, doi: 10.6633/IJNS.201505.17(3).06.
- [102] U.S. Food and Drug Administration, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," 2018. [Online]. Available: <https://www.fda.gov/media/119933/download>
- [103] S. B. Schwartz, "Medical device cybersecurity through the FDA lens." Baltimore, MD: USENIX Association, 2018.
- [104] U.S. Food and Drug Administration, "Postmarket Management of Cybersecurity in Medical Devices," pp. 1–30, 2016. [Online]. Available: <https://www.fda.gov/media/95862/download>
- [105] L. Zhang, K. J. Wang, H. Chen, and Z. H. Mao, "Internet of Brain: Decoding Human Intention and Coupling EEG Signals with Internet Services," in *Proceedings of International Conference on Service Science, ICSS*. IEEE, oct 2016, pp. 172–179, doi: 10.1109/ICSS.2016.32.
- [106] N. R. B. Martins, A. Angelica, K. Chakravarthy, Y. Svidinenko, F. J. Boehm, I. Opris, M. A. Lebedev, M. Swan, S. A. Garan, J. V. Rosenfeld, T. Hogg, and R. A. Freitas, "Human Brain/Cloud Interface," *Frontiers in Neuroscience*, vol. 13, p. 112, mar 2019, doi: 10.3389/fnins.2019.00112.
- [107] R. P. N. Rao, A. Stocco, M. Bryan, D. Sarma, T. M. Youngquist, J. Wu, and C. S. Prat, "A Direct Brain-to-Brain Interface in Humans," *PLoS ONE*, vol. 9, no. 11, p. e111332, nov 2014, doi: 10.1371/journal.pone.0111332.
- [108] A. Ramakrishnan, P. J. Ifft, M. Pais-Vieira, Y. W. Byun, K. Z. Zhuang, M. A. Lebedev, and M. A. Nicolelis, "Computing Arm Movements with a Monkey Brainer," *Scientific Reports*, vol. 5, no. 1, p. 10767, sep 2015, doi: 10.1038/srep10767.
- [109] Emotiv, "Emotiv Cortex API." [Online]. Available: <https://emotiv.github.io/cortex-docs/{#}introduction>
- [110] I. Stelliós, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Sur-*

- veys & Tutorials, vol. 20, no. 4, pp. 3453–3495, 2018, doi: 10.1109/COMST.2018.2855563.
- [111] Open Web Application Security Project, “OWASP Internet of Things Project.” [Online]. Available: <https://www.owasp.org/index.php/OWASP{ }Internet{ }of{ }Things{ }Project>
- [112] A. Botta, W. de Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things: A survey,” *Future Generation Computer Systems*, vol. 56, pp. 684–700, mar 2016, doi: 10.1016/J.FUTURE.2015.09.021.
- [113] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, “Cloud computing security challenges & solutions-A survey,” in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC 2018*. IEEE, jan 2018, pp. 347–356, doi: 10.1109/CCWC.2018.8301700.
- [114] S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, nov 2016, doi: 10.1016/J.JNCA.2016.09.002.
- [115] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead,” *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, apr 2017, doi: 10.1016/J.JNCA.2017.02.001.
- [116] P. Zhang, M. Zhou, and G. Fortino, “Security and trust issues in Fog computing: A survey,” *Future Generation Computer Systems*, vol. 88, pp. 16–27, nov 2018, doi: 10.1016/J.FUTURE.2018.05.008.
- [117] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges,” *Future Generation Computer Systems*, vol. 78, pp. 680–698, jan 2018, doi: 10.1016/J.FUTURE.2016.11.009.
- [118] R. Mahmud, R. Kotagiri, and R. Buyya, “Fog Computing: A Taxonomy, Survey and Future Directions.” Springer, Singapore, 2018, pp. 103–130, doi: 10.1007/978-981-10-5861-5\_5.
- [119] N. Amara, H. Zhiqi, and A. Ali, “Cloud Computing Security Threats and Attacks with Their Mitigation Techniques,” in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, oct 2017, pp. 244–251, doi: 10.1109/CyberC.2017.37.
- [120] M. A. L. Nicolelis, “Actions from thoughts,” *Nature*, vol. 409, no. 6818, pp. 403–407, 2001, doi: 10.1038/35053191.
- [121] “The BRAIN Initiative.” [Online]. Available: <https://braininitiative.nih.gov/>
- [122] J. Illes, S. Weiss, J. Bains, J. A. Chandler, P. Conrod, Y. De Koninck, L. K. Fellows, D. Groetzinger, E. Racine, J. M. Robillard, and M. B. Sokolowski, “A Neuroethics Backbone for the Evolving Canadian Brain Research Strategy,” *Neuron*, vol. 101, no. 3, pp. 370–374, feb 2019, doi: 10.1016/j.neuron.2018.12.021.
- [123] “Canadian Brain Research Strategy.” [Online]. Available: <https://canadianbrain.ca/>
- [124] “Human Brain Project.” [Online]. Available: <https://www.humanbrainproject.eu/en/>
- [125] “Brain/Neural Computer Interaction project.” [Online]. Available: <http://bncl-horizon-2020.eu/>
- [126] C. Brunner, N. Birbaumer, B. Blankertz, C. Guger, A. Kübler, D. Mattia, J. d. R. Millán, F. Miralles, A. Nijholt, E. Opisso, N. Ramsey, P. Salomon, and G. R. Müller-Putz, “BNCI Horizon 2020: towards a roadmap for the BCI community,” *Brain-Computer Interfaces*, vol. 2, no. 1, pp. 1–10, jan 2015, doi: 10.1080/2326263X.2015.1008956.
- [127] M.-m. Poo, J.-l. Du, N. Ip, Z.-Q. Xiong, B. Xu, and T. Tan, “China Brain Project: Basic Neuroscience, Brain Diseases, and Brain-Inspired Computing,” *Neuron*, vol. 92, no. 3, pp. 591–596, nov 2016, doi: 10.1016/j.neuron.2016.10.050.
- [128] “Brain/MINDS project.” [Online]. Available: <https://brainminds.jp/en/>
- [129] IETF, “The Transport Layer Security (TLS) Protocol Version 1.3,” 2018. [Online]. Available: <https://tools.ietf.org/html/rfc8446>
- [130] IETF, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap,” 2011. [Online]. Available: <https://tools.ietf.org/html/rfc6071>
- [131] ISO, “ISO/IEC 27001 Information security management.” [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>
- [132] NIST, “Cybersecurity Framework.” [Online]. Available: <https://www.nist.gov/cyberframework>
- [133] HL7 International, “Health Level Seven.” [Online]. Available: <https://www.hl7.org/>
- [134] T. Vaughan, D. Mcfarland, G. Schalk, W. Sarnacki, D. Krusienski, E. Sellers, and J. Wolpaw, “The Wadsworth BCI Research and Development Program: At Home With BCI,” *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 14, no. 2, pp. 229–233, jun 2006, doi: 10.1109/TNSRE.2006.875577.
- [135] H. Francis, “The Global Superorganism: an evolutionary-cybernetic model of the emerging network society,” *Social Evolution & History*, vol. 6, no. 1, 2007.
- [136] L. Iandoli, M. Klein, and G. Zollo, “Enabling On-Line Deliberation and Collective Decision-Making through Large-Scale Argumentation,” *International Journal of Decision Support System Technology*, vol. 1, no. 1, pp. 69–92, jan 2009, doi: 10.4018/jdsst.2009010105.
- [137] A. L. Luvizotto, A. Mura, R. Prueckl, and U. Bernardet, “Disembodied and Collaborative Musical Interaction in the Multimodal Brain Orchestra,” in *NIME '10: Proceedings of the international conference on New Interfaces for Musical Expression*, 2010.
- [138] E. M. Mugler, C. A. Ruf, S. Halder, M. Bensch, and A. Kubler, “Design and Implementation of a P300-Based Brain-Computer Interface for Controlling an Internet Browser,” *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 18, no. 6, pp. 599–609, dec 2010, doi: 10.1109/TNSRE.2010.2068059.
- [139] J. L. Sirvent, J. M. Azorín, E. Iáñez, A. Úbeda, and E. Fernández, “P300-Based Brain-Computer Interface for Internet Browsing,” in *Trends in Practical Applications of Agents and Multiagent Systems*. Springer, Berlin, Heidelberg, 2010, pp. 615–622, doi: 10.1007/978-3-642-12433-4\_72.
- [140] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: non-invasive security for implantable medical devices,” *Proceedings of the ACM SIGCOMM 2011*, vol. 41, no. 4, pp. 2–13, 2011, doi: 10.1145/2018436.2018438.
- [141] J. E. O’Doherty, M. A. Lebedev, P. J. Ifft, K. Z. Zhuang, S. Shokur, H. Bleuler, and M. A. L. Nicolelis, “Active tactile exploration using a brain-machine-brain interface,” *Nature*, vol. 479, no. 7372, pp. 228–231, nov 2011, doi: 10.1038/nature10489.
- [142] Y. Wang and T.-P. Jung, “A Collaborative Brain-Computer Interface for Improving Human Performance,” *PLoS ONE*, vol. 6, no. 5, p. e20422, may 2011, doi: 10.1371/journal.pone.0020422.
- [143] A. Bernstein, M. Klein, and T. W. Malone, “Programming the global brain,” *Communications of the ACM*, vol. 55, no. 5, p. 41, may 2012, doi: 10.1145/2160718.2160731.
- [144] M. P. Eckstein, K. Das, B. T. Pham, M. F. Peterson, C. K. Abbey, J. L. Sy, and B. Giesbrecht, “Neural decoding of collective wisdom with multi-brain computing,” *NeuroImage*, vol. 59, no. 1, pp. 94–108, jan 2012, doi: 10.1016/J.NEUROIMAGE.2011.07.009.
- [145] T. Yu, Y. Li, J. Long, and Z. Gu, “Surfing the internet with a BCI mouse,” *Journal of Neural Engineering*, vol. 9, no. 3, p. 036012, jun 2012, doi: 10.1088/1741-2560/9/3/036012.
- [146] R. Poli, C. Cinel, A. Matran-Fernandez, F. Sepulveda, and A. Stoica, “Towards cooperative brain-computer interfaces for space navigation,” in *Proceedings of the 2013 international conference on Intelligent user interfaces - IUI '13*. New York, New York, USA: ACM Press, 2013, p. 149, doi: 10.1145/2449396.2449417.
- [147] S.-S. Yoo, H. Kim, E. Filandrianos, S. J. Taghados, and S. Park, “Non-Invasive Brain-to-Brain Interface (BBI): Establishing Functional Links between Two Brains,” *PLoS ONE*, vol. 8, no. 4, p. e60410, apr 2013, doi: 10.1371/journal.pone.0060410.
- [148] P. Yuan, Y. Wang, X. Gao, T.-P. Jung, and S. Gao, “A Collaborative Brain-Computer Interface for Accelerating Human Decision Making,” in *International Conference on Universal Access in Human-Computer Interaction*. Springer, Berlin, Heidelberg, 2013, pp. 672–681, doi: 10.1007/978-3-642-39188-0\_72.
- [149] C. Grau, R. Ginhoux, A. Riera, T. L. Nguyen, H. Chauvat, M. Berg, J. L. Amengual, A. Pascual-Leone, and G. Ruffini, “Conscious Brain-to-Brain Communication in Humans Using Non-Invasive Technologies,” *PLoS ONE*, vol. 9, no. 8, p. e105225, aug 2014, doi: 10.1371/journal.pone.0105225.
- [150] C. Kapeller, R. Ortner, G. Krausz, M. Bruckner, B. Z. Allison, C. Guger, and G. Edlinger, “Toward Multi-brain Communication: Collaborative Spelling with a P300 BCI,” in *International Conference on Augmented Cognition*. Springer, Cham, 2014, pp. 47–54, doi: 10.1007/978-3-319-07527-3\_5.
- [151] R. Poli, D. Valeriani, and C. Cinel, “Collaborative Brain-Computer Interface for Aiding Decision-Making,” *PLoS ONE*, vol. 9, no. 7, pp. 1–22, jul 2014, doi: 10.1371/journal.pone.0102693.

- [152] C. B. Simmons, S. G. Shiva, H. Bedi, and D. Dasgupta, "AVOIDIT: A Cyber Attack Taxonomy," in *9th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'14)*, 2014, pp. 2–12.
- [153] S. N. Abdulkader, A. Atia, and M.-S. M. Mostafa, "Brain computer interfacing: Applications and challenges," *Egyptian Informatics Journal*, vol. 16, no. 2, pp. 213–230, jul 2015, doi: 10.1016/J.EIJ.2015.06.002.
- [154] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
- [155] A. Hernández, "Brain waves surfing - (in)security in eeg (electroencephalography) technologies," DEF CON 23. [Online]. Available: <https://www.youtube.com/watch?v=c7FMVb{ }5SBM>
- [156] M. Kyriazis, "Systems neuroscience in focus: from the human brain to the global brain?" *Frontiers in Systems Neuroscience*, vol. 9, p. 7, feb 2015, doi: 10.3389/fnsys.2015.00007.
- [157] M. Naveed, S. Kamara, and C. V. Wright, "Inference Attacks on Property-Preserving Encrypted Databases," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*. New York, New York, USA: ACM Press, 2015, pp. 644–655, doi: 10.1145/2810103.2813651.
- [158] S. Sicari, A. Rizzardi, D. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, jan 2015, doi: 10.1016/J.COMNET.2014.11.008.
- [159] A. Stocco, C. S. Prat, D. M. Losey, J. A. Cronin, J. Wu, J. A. Abernethy, and R. P. N. Rao, "Playing 20 Questions with the Mind: Collaborative Problem Solving by Humans Using a Brain-to-Brain Interface," *PLOS ONE*, vol. 10, no. 9, p. e0137303, sep 2015, doi: 10.1371/journal.pone.0137303.
- [160] H. Al-Mefleh and O. Al-Kofahi, "Taking advantage of jamming in wireless networks: A survey," *Computer Networks*, vol. 99, pp. 99–124, apr 2016, doi: 10.1016/j.comnet.2016.02.011.
- [161] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," *IEEE Access*, vol. 4, pp. 959–979, 2016, doi: 10.1109/ACCESS.2016.2521727.
- [162] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.
- [163] A. A. Karim, T. Hinterberger, J. Richter, J. Mellinger, N. Neumann, H. Flor, A. Kübler, and N. Birbaumer, "Neural Internet: Web Surfing with Brain Potentials for the Completely Paralyzed," *Neurorehabilitation and Neural Repair*, vol. 20, no. 4, pp. 508–515, dec 2006, doi: 10.1177/1545968306290661.
- [164] G. Li and D. Zhang, "Brain-Computer Interface Controlled Cyborg: Establishing a Functional Information Transfer Pathway from Human Brain to Cockroach Brain," *PLOS ONE*, vol. 11, no. 3, p. e0150667, mar 2016, doi: 10.1371/journal.pone.0150667.
- [165] L. Pycroft, S. G. Boccara, S. L. Owen, J. F. Stein, J. J. Fitzgerald, A. L. Green, and T. Z. Aziz, "Brainjacking: Implant Security Issues in Invasive Neuromodulation," *World Neurosurgery*, vol. 92, pp. 454–462, aug 2016, doi: 10.1016/J.WNEU.2016.05.010.
- [166] A. M. Shabut, K. T. Lwin, and M. A. Hossain, "Cyber attacks, countermeasures, and protection schemes - A state of the art survey," in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*. IEEE, 2016, pp. 37–44, doi: 10.1109/SKIMA.2016.7916194.
- [167] M. Yu, N. Kaongoen, and S. Jo, "P300-BCI-based authentication system," in *4th International Winter Conference on Brain-Computer Interface, BCI 2016*. IEEE, feb 2016, pp. 1–4, doi: 10.1109/IWW-BCI.2016.7457443.
- [168] T. Ye, L. Zhang, L. Wang, and X. Li, "An Empirical Study on Detecting and Fixing Buffer Overflow Bugs," in *2016 IEEE International Conference on Software Testing, Verification and Validation (ICST)*. IEEE, apr 2016, pp. 91–101, doi: 10.1109/ICST.2016.21.
- [169] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On Threat Modeling and Mitigation of Medical Cyber-Physical Systems," in *Proceedings - 2017 IEEE 2nd International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2017*. IEEE, jul 2017, pp. 114–119, doi: 10.1109/CHASE.2017.69.
- [170] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, aug 2018, doi: 10.1109/JIOT.2017.2767291.
- [171] S. He, T. Yu, Z. Gu, and Y. Li, "A hybrid BCI web browser based on EEG and EOG signals," in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, jul 2017, pp. 1006–1009, doi: 10.1109/EMBC.2017.8036996.
- [172] M.-P. Hosseini, D. Pompili, K. Elisevich, and H. Soltanian-Zadeh, "Optimized Deep Learning for EEG Big Data and Seizure Prediction BCI via Internet of Things," *IEEE Transactions on Big Data*, vol. 3, no. 4, pp. 392–404, dec 2017, doi: 10.1109/TBDATA.2017.2769670.
- [173] W. Lee, S. Kim, B. Kim, C. Lee, Y. A. Chung, L. Kim, and S.-S. Yoo, "Non-invasive transmission of sensorimotor information in humans using an EEG/focused ultrasound brain-to-brain interface," *PLOS ONE*, vol. 12, no. 6, p. e0178476, jun 2017, doi: 10.1371/journal.pone.0178476.
- [174] M. E. M. Mashat, G. Li, and D. Zhang, "Human-to-human closed-loop control based on brain-to-brain interface and muscle-to-muscle interface," *Scientific Reports*, vol. 7, no. 1, p. 11001, dec 2017, doi: 10.1038/s41598-017-10957-z.
- [175] W. G. de Oliveira Júnior, J. M. de Oliveira, R. Munoz, and V. H. C. de Albuquerque, "A proposal for Internet of Smart Home Things based on BCI system to aid patients with amyotrophic lateral sclerosis," *Neural Computing and Applications*, pp. 1–11, oct 2018, doi: 10.1007/s00521-018-3820-7.
- [176] Open Web Application Security Project, "Top 10-2017 Top 10 - OWASP," 2017. [Online]. Available: <https://www.owasp.org/index.php/Top{ }10-2017{ }Top{ }10>
- [177] A. Saboor, A. Rezeika, P. Stawicki, F. Gemblar, M. Benda, T. Grunenberg, and I. Volosyak, "SSVEP-Based BCI in a Smart Home Scenario," in *International Work-Conference on Artificial Neural Networks*. Springer, Cham, 2017, pp. 474–485, doi: 10.1007/978-3-319-59147-6\_41.
- [178] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber Security Threats to IoT Applications and Service Domains," *Wireless Personal Communications*, vol. 95, no. 1, pp. 169–185, jul 2017, doi: 10.1007/s11277-017-4434-6.
- [179] A. Umair, U. Ashfaq, and M. G. Khan, "Recent Trends, Applications, and Challenges of Brain-Computer Interfacing (BCI)," *International Journal of Intelligent Systems and Applications*, vol. 9, no. 2, pp. 58–65, feb 2017, doi: 10.5815/ijisa.2017.02.08.
- [180] P. Chaudhary and R. Agrawal, "Emerging Threats to Security and Privacy in Brain Computer Interface," *International Journal of Advanced Studies of Scientific Research*, vol. 3, no. 12, pp. 340–344, 2018. [Online]. Available: <https://ssrn.com/abstract=3326692>
- [181] C. G. Coogan and B. He, "Brain-Computer Interface Control in a Virtual Reality Environment and Applications for the Internet of Things," *IEEE Access*, vol. 6, pp. 10840–10849, 2018, doi: 10.1109/ACCESS.2018.2809453.
- [182] A. Costin and J. Zaddach, "IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies," in *BlackHat USA*, 2018. [Online]. Available: <https://www.blackhat.com/us-18/briefings/schedule/{ }#iot-malware-comprehensive-survey-analysis-framework-and-case-studies-11525>
- [183] K. Fu and W. Xu, "Risks of trusting the physics of sensors," *Communications of the ACM*, vol. 61, no. 2, pp. 20–23, jan 2018, doi: 10.1145/3176402.
- [184] R. A. Hyde, M. Y. Ishikawa, E. C. Leuthardt, M. A. Smith, and L. L. Wood Jr, "Secure operation of implanted device," U.S. Patent US9999776B2, 2018. [Online]. Available: <https://pdfpiw.uspto.gov/piw?Docid=9999776>
- [185] M. Ienca, P. Haselager, and E. J. Emanuel, "Brain leaks and consumer neurotechnology," *Nature Biotechnology*, vol. 36, no. 9, pp. 805–810, 2018, doi: 10.1038/nbt.4240.
- [186] S. José and R. Méndez, "Modeling actuations in BCI-O," in *Proceedings of the 8th International Conference on the Internet of Things - IOT '18*. New York, New York, USA: ACM Press, 2018, pp. 1–6, doi: 10.1145/3277593.3277914.
- [187] J. Katona, T. Ujbanyi, G. Sziladi, and A. Kovari, "Electroencephalogram-Based Brain-Computer Interface for Internet of Robotic Things," in *Cognitive Infocommunications, Theory and Applications*. Springer, Cham, 2019, ch. 12, pp. 253–275, doi: 10.1007/978-3-319-95996-2\_12.
- [188] G. Kirubavathi and R. Anitha, "Structural analysis and detection of android botnets using machine learning techniques," *International*

- Journal of Information Security*, vol. 17, no. 2, pp. 153–167, apr 2018, doi: 10.1007/s10207-017-0363-3.
- [189] F. Laport, F. J. Vazquez-Araujo, P. M. Castro, A. Dapena, F. Laport, F. J. Vazquez-Araujo, P. M. Castro, and A. Dapena, “Brain-Computer Interfaces for Internet of Things,” *Proceedings*, vol. 2, no. 18, p. 1179, sep 2018, doi: 10.3390/proceedings2181179.
- [190] H. Lu, H. Kim, Y. Li, and Y. Zhang, “BrainNets: Human Emotion Recognition Using an Internet of Brian Things Platform,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, jun 2018, pp. 1313–1316, doi: 10.1109/IWCMC.2018.8450382.
- [191] V. A. Maksimenko, A. E. Hramov, N. S. Frolov, A. Lüttjohann, V. O. Nedaivovov, V. V. Grubov, A. E. Runnova, V. V. Makarov, J. Kurths, and A. N. Pisarchik, “Increasing Human Performance by Sharing Cognitive Load Using Brain-to-Brain Interface,” *Frontiers in Neuroscience*, vol. 12, p. 949, dec 2018, doi: 10.3389/fnins.2018.00949.
- [192] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, “Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks,” *IEEE Communications Surveys and Tutorials*, vol. 20, no. 2, pp. 1361–1396, 2018, doi: 10.1109/COMST.2017.2781126.
- [193] H. Rathore, C. Fu, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, and Z. Yu, “Multi-layer security scheme for implantable medical devices,” *Neural Computing and Applications*, pp. 1–14, oct 2018, doi: 10.1007/s00521-018-3819-0.
- [194] A. Saboor, F. Gembler, M. Benda, P. Stawicki, A. Rezeika, R. Grichnik, and I. Volosyak, “A Browser-Driven SSVEP-Based BCI Web Speller,” in *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, oct 2018, pp. 625–630, doi: 10.1109/SMC.2018.00115.
- [195] B. Xu, W. Wang, Q. Hao, Z. Zhang, P. Du, T. Xia, H. Li, and X. Wang, “A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device,” *IEEE Access*, vol. 6, pp. 72 862–72 869, 2018, doi: 10.1109/ACCESS.2018.2881447.
- [196] X. Zhang, L. Yao, S. Zhang, S. Kanhere, M. Sheng, and Y. Liu, “Internet of Things Meets Brain-Computer Interface: A Unified Deep Learning Framework for Enabling Human-Thing Cognitive Interactivity,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2084–2092, apr 2019, doi: 10.1109/JIOT.2018.2877786.
- [197] S. Saha, K. A. Mamun, K. Ahmed, R. Mostafa, G. R. Naik, A. Khandoker, S. Darvishi, and M. Baumert, “Progress in Brain Computer Interfaces: Challenges and Trends,” jan 2019. [Online]. Available: <http://arxiv.org/abs/1901.03442>
- [198] T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices – A Review,” *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2019, doi: 10.1109/COMST.2019.2914094.