Cyberneurosecurity

Nadine Liv and Dov Greenbaum

1 Introduction

Decades ago, as biological labs came into the internet age, they were subject to increased cybersecurity threats to their computing infrastructure. These attacks often occurred either directly through network infrastructure such as unsecured wifi, through email phishing attacks targeted to unsuspecting lab members, or through infected shared disks. For the most part, these early efforts to infiltrate the computing infrastructure of life science laboratories, both commercial and academic, were either designed to maliciously disable lab computers or to extract information and intellectual property for profit [1].

The area of research that grew out of the need to deal with the issues of cybersecurity as they related primarily to health science research ultimately became known as cyberbiosecurity (or alternatively as biocybersecurity) [2]. Much of the early research in this emerging field focused predominantly on securing the interface between the biosciences and cyberspace, principally in terms of protecting biological research from cybersecurity threats, but also in employing biological methods to the world of cybersecurity [3–5] and in employing cybersecurity methods in the world of biology [6].

N. Liv
Meitar Liquornik Geva Leshem Tal, Ramat Gen, Israel

Harry Radzyner Law School, Reichman University, Herzliya, Israel

D. Greenbaum (✉)
Harry Radzyner Law School, Reichman University, Herzliya, Israel

Zvi Meitar Institute for Legal Implications of Emerging Technologies, Reichman University, Herzliya, Israel

Molecular Biophysics and Biochemistry, Yale University, New Haven, CT, USA
e-mail: dov.greenbaum@runi.ac.il

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
V. Dubljević, A. Coin (eds.), *Policy, Identity, and Neurotechnology*, Advances in Neuroethics, https://doi.org/10.1007/978-3-031-26801-4_13

Recently, this area of research has become even more relevant to genomic researchers when it was shown that malevolent individuals could target more specific vulnerabilities at the intersection between cyberspace and biology such as genomic engineering. Consider the possibility that malware could masquerade as common academic bioinformatic software such as codon optimization tools. These tools could be employed by unsuspecting researchers to suggest the creation of physical DNA sequences designed to wreak havoc in unwary research systems. Or consider the possibility that a naive researcher's interactions with a commercial DNA producer could be hijacked and the formerly benign DNA code that said researcher intended to order for her experiment is replaced with a malicious sequence, the properties of that malicious sequence potentially further obfuscated via cryptographic tools. Once that DNA strand is returned to our unsuspecting researcher and integrated into her genomic research systems, that DNA, perhaps coding for some toxic protein, could wreak havoc. Proof of concept of such an attack has already been shown [7]. The nature of these types of software and DNA threats are exacerbated by the reality that the necessary tools for their implementation are generally publicly available. Similarly, software masquerading as benign or an upgrade to a BCI may in fact contain malicious code that could be harmful to the user and/or the people around them.

This paper is meant to be an introductory look into the emerging field of cyberneurosecurity (or neurocybersecurity), a subfield within the incipient field of cybersbioecurity. The paper is presented as follows: We first present the field of cyberbiosecurity noting in particular how that term represents a unique field. We then present how the field of cyberneurosecurity is situated within the larger cyberbiosecurity field. Following these definitions, we present brain–computer interfaces (BCIs), the primary source of hackable electronics when discussing cyberneurosecurity. Within the field of BCIs, we discuss issues specific to their security, as well as the neurorights that have arisen as a result of the increasing advancements within BCI technology. We counter some of that discussion of advancements with an acknowledgement of the pervasiveness of neurohype, i.e., neuro related technologies that are currently more fiction than reality. Although not necessarily a technology that will be implemented in the immediate or near future, the possibility of uploading consciousness to an AI machine, an idea that might or might not fall within the aforementioned concept of neurohype, could also conceivably raise many interesting and novel concerns in the field of cyberneurosecurity. Finally, with all of these aspects presented, we provide the reader with a thorough discussion of the actual field of cyberneurosecurity, including discussions of specific cases as well as potential countermeasures to the cyber threats on neurotechnologies.

2 Cyberbiosecurity

Given these fears, one early definition of cyberbiosecurity defined the nascent field as one devoted to the understanding of "the vulnerabilities to unwanted surveillance, intrusions and malicious and harmful activities which can occur *within or at the interface* of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures, to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience" [8]. It has been noted by cyberbiosecurity's early promoters that the landscape for cyberbiosecurity would ultimately evolve rapidly and that this definition would eventually need updating.

Part of that updating is the goal of this particular chapter. Concerns in the area of cyberbiosecurity have long grown past just the aforementioned field of genomics. There are equally, if not greater concerns that arise in the area of neurotechnologies. Just like researchers in the field of bioethics found it necessary to include a subfield devoted particularly to neuroethics in the early part of the century [9], we think the time is right to develop and describe a subfield in cyberbiosecurity devoted wholly to neurotechnologies. Overall, this is what we refer to here as the subfield of cyberneurosecurity. Like cyberbiosecurity, we distinguish cyberneurosecurity from the cybersecurity for neuroscience and neurosecurity [10] in that this field is broader, incorporating like cyberbiosecurity, issues relating to neurorights, neuroprivacy, and neuroethics, as well as the potential future uses of neuroscience technologies in the service of cybersecurity and/or hacking. Cyberneurosecurity is not only interested in issues arising at the intersection of brain–computer interfaces, but also with regard to the attacks in future brain to brain (BtB) communications [11] as well as brain to internet communication [12].

In the area of cyberneurosecurity, an unauthorized hack can project force onto an individual, or read the thoughts of an individual [13–15], either locally or remotely [16]. These possibilities [17] take the cybersecurity concerns to a radically different level than those of cyberbiosecurity.

In addition to being somewhat distinct from discussions on cyberbiosecurity, we believe the cyberneurosecurity is a unique and distinct subfield of cyberbiosecurity because of the personal nature of these potential attacks against the human brain, as described herein. Such attacks can lead to both direct and indirect harm with profound ethical and legal implications; many of these harms, as described herein, are unique to the world of neuroscience. For example, researchers have noted that the misuse of neural devices for malicious purposes may not only threaten users' physical security, but also it can influence the user's behavior and alter their sense of identity and personhood. Additionally, in contrast to many other criminal activities associated with biological devices, the attack on neurodevices can create an extreme sense of anxiety and fear and otherwise severely affect the overall mental state of the targeted individual [18]. Such attacks violate centrally human moral values of autonomy, free will, and self-determination [19].

3 Brain–Computer Interfaces

We define this subfield as mostly interested in the neuroscience tools that can read and write to the brain such as brain–machine/computer interfaces (BMI, or BCIs). BCIs have been around for almost half a century, but only recently have there been an uptick in the academic literature relating to their related cybersecurity concerns [20]. This is disconcerting: Brain to Internet (B2I) technology is already available [21], and as some suggest, BCI technology will only become more pervasive within the general public in the coming decade [22]. Already cheap open source devices are readily purchasable.

BCIs can be broadly defined as devices that record, process, analyze, and/or modify brain activity. BCIs directly connect the brain, invasively via surgery, partially invasively via electrocorticography (ECog or iEEG), or wholly non-invasively via EEG or fMRI, to a computer. In some instances, BCIs only report brain activity, in others, BCIs also effectuate events outside of the user's body, typically circumventing peripheral nerves and sending electro-physiological signals directly to a machine, such as a prothesis [23]. BCIs may also mediate incoming signals to the brain. More practically, BCIs can be used for a host of applications [24]. These include gaming [25] and other recreational activities [26], health and medical, and increasingly biometric authentication [27].

BCIs clearly fall within the category of "comingled life sciences… and cyber" set forth in the definition of cyberbiosecurity above. However, as a result of their unique integration of neuroscience and technology, BCIs are at the forefront of the subfield of cyberneurosecurity risks, and as BCIs evolve, cybersecurity concerns relating especially to neuroscience will continue to evolve as well.

4 Neurosecurity

Notably, some have already described components of cyberneurosecurity within what is known as neurosecurity, i.e., the protection of the confidentiality, integrity, and availability of neural devices and their data from malicious third parties [28]. Neurosecurity can be additionally defined as the employment of knowledge as to how the brain functions when employing cybersecurity tools [29, 30]. Neurosecurity has also been defined as the use of neuroscience for national defense: "Creating resilient soldiers (to stress, fatigue, overload)… [or] Developing rapid training and learning techniques" [31].

Some outcomes of the failure to recognize the value of pursuing neurosecurity goals have already been documented to include the creation of software that has been shown to be able to infiltrate BCI systems to extract privacy-related information [32], the hijacking of prosthetic limbs to create damage or limit the motility of a disabled individual (sometimes termed the failure of availability), the malicious programming of neurostimulation therapy to harm a patient [33, 34]—through tools like transcranial magnetic stimulation, transcranial direct current stimulation, deep brain stimulation, sensory prosthetic and orthotic implants transcranial Doppler or direct cortical electrical stimulation, the interception and reprogramming of signaling between a BCI and an external object [35], and the eavesdropping on a brain implant's signals to reveal private information (sometimes termed a breach of integrity) [28], including discrete pieces of private information such as a personal identification code (PIN) [36].

In contrast to neurosecurity, cyberneurosecurity, as we see it, is both broader and more encompassing while also narrower. To wit: more than just cybersecurity attacks on the BCIs to extract information, hijack prosthetic limbs, manipulate output or even to introduce ransomware that serves the connection between a user and their prosthetic, cyberneurosecurity also includes the manipulation of BCIs by their own users. This manipulation is less for malicious purposes, but rather to override safety settings or other built-in limitations. These hacks can be just as dangerous to the user, as well as to those in their vicinity as malicious attacks, but because the hacker isn't unauthorized, they are typically not included in the neurosecurity discussion.

For example, consider the prospect of medical BCIs being modified to provide otherwise unintended and unfair benefits to the consumers of these devices, such as enhancing memory or cognition. Alternatively, a neuromodulation device could be modified to activate the reward circuitry of the brain potentially resulting in the development of addictive behaviors in the pursuit of desirable sensations or experiences. Already BCIs are being developed to provide for some forms of neuromodulation such as creating enhanced memory and cognition in those experiencing mental decline [37]. However, the same technology designed to bring those who are suffering from deficiencies up to par may, hypothetically also someday provide those at par with extra-human abilities. This potential hacking of a medical BCI for non-medical gains of human enhancement [38, 39] will become more likely as BCIs become more commonplace and consumer grade technologies become more promising [40]. Another area of interest within cyberneurosecurity is the topic of neurorights and the corresponding obligations that arise from them.

5 Neurorights

In general, the hacking of neurodevices to manipulate a patient impinges on the patient's autonomy. This manipulation may occur via many paths, including eliciting emotions, manipulating decision-making and preferences, and manipulating memories. In addition, an attack on BCIs can also impinge on other emerging cognitive rights of the user/consumer/patient. These neurorights are a relatively new academic legal area [41]. Notably, neurorights are not explicitly reflected in the vast majority of national constitutions or international legal instruments, with the exception of Chile and potentially Spain [42].

Some have argued that the neurohype regarding products that are far from available has fed the efforts to develop neurorights long before they are necessary. Without knowing exactly was emerging technologies which are capable of the issues relating to neurorights are not yet ripe and perhaps even ultimately misguided depending on how the relevant technologies actually develop and mature. This is especially problematic, according to critics, for countries like Chile and Spain which are zealously taking the broad ideas developing within the neurorights community and turning them into hard and fast legal rights, rules, and regulations. Ultimately, these premature efforts could stifle innovation rather than promoting its development.

One of these rights is the long standing right to cognitive liberty which outlines the right of each individual to be able to think autonomously and independently without outside interference [43]. Cognitive liberty is an umbrella-like right that incorporates many of the standard rights of freedom of speech, freedom of religion, and freedom of choice. Thus, the right to cognitive liberty is the right to make your own choices, unencumbered by the unknown or undesired influence of others: it “guarantees an individual’s sovereignty over her mind and entails the permission to both use and refuse neuro-enhancement” [44]. Accordingly, when third parties hack a neurodevice to manipulate the mental states of an individual, they have violated that individual’s cognitive liberty.

Notably, the concept of cognitive liberty also suggests that an individual ought to have the right to self-employ mind enhancing neurodevices as well. However, this neuroenhancement is constrained by the obligation not to harm others. This is a real fear when a user of a BCI hacks their own device to operate it outside of manufacturers’ safety constraints, one of the potential interests of the field of cyberneurosecurity.

Other neurorights that might be affected by malicious attacks on neurodevices are the right to mental privacy, the right to mental integrity, and the right to psychological continuity [45]. The right to mental privacy grants individuals the right to be free from third parties peering into their thoughts and emotions, e.g., via a hacked BCI.

The right to mental integrity is the individual’s right to have control over their own thoughts and the right to prevent third parties from intruding into their brain and introducing fake information. Again, such an intrusion can occur via a hacked BCI that provides input to the brain. Mental integrity can be further impinged via a cyberneurosecurity attack on a BCI that harms neurological tissue. In this case there is a fear that such an attack could manipulate or erase memories that provide individuals with their weltanschauung and their personal autobiographical record.

The right to psychological continuity similarly refers to the right to not have foreign ideas and memories implanted into an individual’s mind. Anything that harms or changes an individual’s particular mental sense of self is a potential violation of this right. Any alterations in mental states may affect areas critical to a person’s identity and personality [45]. Some have countered that this right particularly highlights many of the concerns with neurorights proposals: Broad statements of rights like these can be misleading or confusing and even vulnerable to counterclaims. Consider the reality that humans are always having foreign ideas and memories placed in our minds simply through daily interactions with reality. Any new idea can affect our mental sense of self. Arguably, the whole process of education would seem to be a problem with regard to the concept of psychological continuity and yet few would suggest that we should disincentivize education and the learning of new ideas that can change our outlook and mindset.

However, even within the scope of these rights, states can also arguably limit an individual’s right to waive other countervailing rights, for example, by enforcing the right of cognitive liberty to prevent a user from hacking their own BCI. Legally, while most modern states allow for self-determinism and the ability of each citizen to decide for themselves who they are, there are also aspects of paternalism within the modern state that will typically step in to prevent self-harm or activities that can harm others.

6 Neurohype?

In many areas of neurotechnologies, there is a concern that much of the ethical, legal, and social issues raised are associated with technologies that are improbable and unlikely; i.e., hype. This concern is often referred to as neurohype, the idea that the lay public is often presented with technological claims regarding neuroscience that are beyond the actual capabilities of the technology, or that authors of various articles on the subject often buy into the hype and pontificate about technologies and their concerns that are years away from reality, if ever reality at all [46]. To some degree, some of this neurohype narrative arises out of a failure in science communication. Many researchers in the neuroscience field are themselves influenced by science fiction to pursue and create new neuroscience realities emulating the fictional accounts and they could end up communicating their research as similar to the fictional technologies. And, to their credit, much of what neuroscientists can accomplish today was arguably science fiction a decade ago [47].

To this end, there may be a concern that many of the issues raised by cyberneurosecurity are themselves unripe, resulting from technology that is merely neurohype, conflating science fiction for reality [46, 48]. In particular, some may think that claims about what is and what isn't possible in regard to hacking technology like BCIs overstate the concerns and create problems where none yet exists. As such while many of the issues mentioned herein are associated with proofs of concept, neurohype still remains a potential caveat on the following assessment of cyberneurosecurity.

7 Cyberneurosecurity: How Cyberbiosecurity Specifically Applies to BCIs

Their 50 years of development notwithstanding, the modern version of brain–computer interface technologies (EEGs themselves were developed nearly a century ago [49]) continues to evolve. As they do, BCIs will continue to bring benefits to the field of medicine, where they are used to diagnose medical conditions, aid in rehabilitation, or control prostheses [50]. Data from these devices can become accessible or manipulatable through a hack. In other cases, the hacker can potentially control, the movement, emotion, or even the brain functions of the target. In worst case scenarios, hacking these devices can cause long-term damage to the brain or the individual, and even death.

Data transmitted from the brain can be collected and interpreted to provide an increasing amount of actionable information about a patient. In general, medical devices are often not the best protected against cyberattacks as they often offer little encryption and employ default passwords to allow for easy interfacing with existing hospital infrastructure [51, 52]. Customers and patients typically are uninterested in encrypting their data: "Given a choice between dancing pigs and security, users will pick dancing pigs every time" [53].

This is especially the case in neurotechnologies where latency between BCI and the end result (e.g., the movement of a prosthetic) is already high. Encryption and decryption would only serve to increase that undesirable latency. Further, encryption draws power that would further limit the battery life of a remote device. Because of these reasons and more, neurotechnological devices in particular and medical devices in general are often seen as vulnerable weak spots in hospital networks [52], making the already increasingly profitable hack of a hospital [54] all the more enticing through providing additional types of personal information: neurological.

Arguably even non-neurotechnological medical technologies also provide opportunities to hack the brain. An insulin pump, for example, or any device that is somehow associated with the peripheral nervous system, is itself potentially an opportunity for a side-channel attack, i.e., by using relevant data collected on the induvial rather than exploiting a design flaw, on the human brain.

Regardless as to whether the BCI is inputting to the brain or collecting output, there are ample opportunities for malicious activities. These activities can result in numerous negative impacts relating to the integrity of medical data collected from the brain or transferred to the brain, the confidentiality of that data, resulting in private and personal information being transferred to third parties, the availability of the data that is generated to manipulate a device, and of course the safety of the user who may suffer from long- or short-term psychological and/or physical damage.

Integrity can also refer to the possibility that third party hackers can effect behavior changes on a person with a BCI by stimulating pleasure and pain sensors every time an activity is desired or undesired. Such technologies are not yet thought to have been developed, but are not necessarily beyond the technological limitations of the current state of the art. In an extreme case, one could imagine the user of a BCI having their pleasure and pain sensors triggered surreptitiously via geolocation sensors, perhaps even creating a situation wherein a person with a brain–machine interface might be limited in where they can and cannot go due to third parties triggering pain regions in the brain every time the individual moves beyond a certain point.

Similarly, availability concerns can also relate to accessibility of the BCI, the devices effectuated by the BCI, such as a prosthetic in the case of a hack. In some cases, a BCI hack may even inhibit access to one's own brain; it has been shown that it is possible to stimulate the brain via a BCI as to affect consciousness [55].

As the term suggests, cyberneurosecurity concerns often arise when hackers employ cybersecurity exploits in the area of neurodevices. These include low complexity attacks such as neural flooding which overstimulate neurons via the BCI, and neuronal jamming which is the impeding the information flow from neurons to BCIs. In this instance, a neuronal jamming attack is like a denial of service (DoS) attack, but with biological parts like neurons in contrast to internet infrastructure. Moderate complex attacks can include such hacks as neuronal scanning, which is like port scanning in a cyberattack, but instead of seeking out internet ports, the attack sequentially maliciously stimulates each BCI associated neuron, one at a time and neuronal selective forwarding, which purposefully inhibits only some data from going from the brain to the BCI or vice versa with the intent of incapacitating the information flow. More sophisticated attacks like neuronal spoofing confuse the brain and/or the BCI by replicating an earlier legitimate neuron behavior, but at a different time or location while a neuronal nonce attack modulates the nature of the attack randomly so that the BCI has difficulty in identifying the malicious actions [56]. In addition to these, there are numerous other types of cyberattacks that can exploit the internet-enabled aspects of a BCI [12] as they could any other medical device internet of things (MDIoT) device [57, 58].

8 BCI Data Hacking

Both in health and in employment, the BCI data collected is more than simply a snapshot of some biometric information. An EEG reading can give an indication about the emotional state of the user at a particular point in time. This information can be accumulated over time to create a detailed profile of the user's emotional states [59].

As per standard cybersecurity protocols, data can be maliciously acted upon either when it is at rest, in transit/motion, or in use [60]. Broadly, in either direction of BCI action, there are at least five instances that represent these different aspects of data. When the goal of the BCI is to output data from the brain, these five instances include:

1. Neural data acquisition wherein neural signals are generated, representing the data in its rawest form
2. Data capture from one of the electrodes associated with the brain
3. The conversion of analog neural signals to digital data. This conversion often also includes the reduction of noise from the raw data, resulting in cleaner and more useful signal
4. Processing and decoding digitized signal, in some cases by way of artificial intelligence, in an effort to extract actionable information from the initial neural impulses and
5. The use of any actionable data is put into practice by way of any external device, such as a prosthetic, or a display showing the processed signal [12]

A BCI system can also go in the reverse direction, effecting an external input on the brain wherein

1. An external input is collected through sensors or other inputs
2. That input is then collected and analyzed, and in some cases, converted into a neural firing pattern
3. That firing pattern is then optimized by assessing which neurons ought to be stimulated and by how much voltage
4. Those parameters are passed on to the device that is in physical contact with the brain
5. And finally, that BCI physically stimulates the brain according to the determined parameters

Potential cyberneurosecurity attacks can include attacks in each of the aforementioned steps, both in acquiring signal and in signaling the brain. Here researchers have documented numerous different types of attacks.

During the data acquisition phase (first or last depending on whether the BCI is for input or output), for example, a hack could falsify external stimuli, or the electrodes could be tricked into receiving inaccurate data such as through subliminal stimulations [61]. In the latter neurostimulation of the brain, it is theorized that the nature of the stimulation could disrupt the parameters of the firing pattern increasing/decreasing the quantity of spikes, their voltage, their dispersion, or other modifications [62].

In some cases, this type of hacking can even cause long-term tissue damage [63]. In other cases changing the parameters of the firing pattern, or even introducing novel firing patterns unrelated to external stimuli can create false perceptions that can result in psychological [64] and even physical [65] concerns.

Other cyberneurosecurity concerns in data acquisition of the BCI signal include jamming attacks which can affect the confidentiality, integrity, and availability of the signal. For example, this malware could prevent the data acquisition component of a BCI from picking up raw signals collected by the electrodes [66]. In conversion of analog to digital signal, there is also the possibility of a cyberneurosecurity attack, especially via malicious malware that could confound the conversion process, or extract the data regarding private thoughts of the user and provide it to a third party [67]. Such technology, while still in its infancy, is already able to decode images from BCI outputs [68–72], or extract other information [32]. Notably different from other digital communications that can be hijacked, often times those using BCIs are particularly vulnerable, e.g., mentally and physically handicapped, and the data that might be transferred between BCIs and other devices may also include particularly private and informative information. Finally, malware can also intervene in the digital to analog conversion of brain stimulation signal, as well as extract data regarding the nature of the neurological treatments.

9 Specific Cases of Cyberneurosecurity Concerns in Medical, Recreational, and Employment Uses of BCI

A typical hacking case that comes up considerably in the literature is that of malicious activity performed against a brain–computer interface in the context of medical care. Prominent in these cases is the fear of a hostile takeover by a cyber-attacker against a brain–computer interface that operates a patient's neuro-prostheses, against their will [73].

Another commonly described concern stems from the misdiagnosis of neurological diseases when neurodevices are hacked and the integrity of information is disrupted and/or misrepresented information is provided in its place [51]. The hacking of this data can also severely impact the privacy and autonomy of the patient. Notably, this hacking need not require that the victim of the hacking even be physically connected to a brain–machine interface such as an EEG. Research has shown that remote brain access is a near-future reality [74].

Private data from BCIs can also be extracted from non-medical contexts. Consider, for example, SmartCap an Australian company that manufactures wearable technologies for monitoring the fatigue of workers in various industries such as truck drivers, miners, and commercial workers [75]. Another similar technology, Life, an EEG-based headband that provides real-time feedback and allows users—e.g., truck drivers—to manage their alertness by sending alerts delivered via a dedicated app linked via Bluetooth and thus reducing the risk involved in their work [76]. Similarly, the Chinese government is funding a project to scan the brain data of workers in various industries. Production line workers, state-owned companies' employees, and high-speed train drivers are required to use headgear with EEG technology that purports to detect changes in emotional states [77]. The project scans brain data to identify signs of depression, anxiety, or anger through artificial intelligence (AI) and businesses adjust themselves accordingly [78]. These are just a few of the many similar technologies available [79].

There is no doubt that the use of BCIs for employer or state surveillance purposes is one of the most worrying dystopian scenarios regarding this technology. However, even in their best light, these applications, while ostensibly monitoring employee engagement in order to improve safety during high-risk tasks and alert employees or supervisors to dangerous physical or mental situations [80], can also be hacked to expose the sensitive and private data collected by the devices to less scrupulous third parties [81].

Regardless of the actual device employed in these employment contexts, in contrast to the medical field with its relatively strict requirements for protecting private patient data, employers have very little if any regulation that requires anything approaching the level of protection within the medical environment, and yet the technology allows them to collect medical grade, or near-medical grade data. That data can be intercepted while it is being collected, transferred, or analyzed. And while the data may be noisier than the data collected in a hospital setting, there is the real possibility of extracting private neurological data.

Even when they are less obligated to limit the nature of data protection, governments and employers are typically regulated with regard to the data that they can collect and analyze. This is not necessarily the case for other industries that are employing nascent BCI technologies. The field of neuromarketing—sometimes known as consumer brain sciences—researches the brain to predict and even manipulate consumer behavior and decision-making [82]. Neurodata is valuable to advertising and marketing bodies due to its potential to identify how and why people respond to different stimuli to better influence consumers [83]. Beyond the concerns that this ability to examine responses and perceptions directly from the brain creates new ethical debates, such as how to set the accepted boundaries of manipulation, the lack of regulation in this recreational use of BCIs is disconcerting, especially as it relates to the safety of collected data.

Similarly, another recreational application for BCIs is the recreational industry itself, specifically in the gaming industry. Third-party brain–computer interface games rely on standard application programming interfaces (API) to gain access to the brain–computer interface. Such application programming interfaces provide unrestricted access to raw EEG signals for brain–computer interface games, and moreover, these games have full control over the stimuli that can be displayed to users. It turns out that attackers can view the content and read the same EEG associated with them [84]. This confidentiality problem is not exclusive to gaming. Most APIs that are used for the development of BCI application grant unrestricted access to data acquired by the brain–computer interface [85].

Specific examples of this technology abound. Aimed at providing a more immersive gaming experience, Valve, a gaming company, has partnered with OpenBCI, a neurotech company responsible for numerous open-source, non-invasive BCI devices [86], and Tobii, an eye-tracking firm [87], to launch a virtual reality (VR) brain–computer interface "Galea" in early 2022 [88]. The company uses brain–computer interface signals to engage the player for a longer period of time by changing the level of difficulty of the game in response to signs of fatigue stress or boredom.

This data can be employed to draw conclusions about the user's preferences. Models of artificial intelligence and machine learning can be trained on the user's brain signals—combined with other biological changes in response to content—allowing organizations to associate specific changes occurring in the user's neural with certain physiological conditions, such as arousal.

Notably, the retail industry has also learned to access neurological information without any devices interacting with the brain. Some refer to aspects of this as biometric psychography, i.e., the use of behavioral and anatomical information such as pupil dilation to measure a person's response to stimuli over time. It can reveal both the physical, mental, and emotional state of a person, and the stimuli that caused him or her to enter that state. In particular, biometric psychography can reveal intimate details about users' preferences and interests. Unlike biometrics, which focuses primarily on identity, biometric psychography focuses on the practice of using biometric data to identify areas of interest, attitudes, and lifestyles related to the user's personality structure [89, 90]. Arguably, although this analysis includes neurological assessments and to some degree, it is based on neurological science, it is likely, by definition, out of the scope of cyberneurosecurity; that is not to say that malicious access to this information need not be protected under a different rubric. However, this neurological information arguably ought still be protected by the aforementioned emerging ideals of neurorights. Regardless as to how data is collected, the underlying principles and morals relating to neurorights stand. One need not interact with the brain biologically to impinge on these rights.

Similarly, while many of the social media platforms we currently use are already influencing user behavior through the implementation of smart algorithms that encourage even without directly interfacing with the brain.

10 Self-Hacking

The use of BCIs for individuals with medical conditions or where their brain function has been impaired is well known [91]. BCIs can also be used to enhance in addition to their restorative powers [92]. And it is not just cognitive enhancement that can be accomplished via a BCI—attached to an exoskeleton it can provide superhuman strength; it can also change a user's mood. Note this hacking could also be used to decrease one's neuroabilities, raising its own set of novel concerns.

There is often a fine line between enhancement/augmentation and therapy [38, 39, 93]. We have long used pharmacological solutions for cognitive enhancement, including caffeine which is readily and widely available. Ought we make a distinction when using a device such as a BCI. Does society believe that it is ethically problematic to appropriate BCI technologies to enhance rather than repair. Some, for example, might question the authenticity of actions that are enabled by enhancing technology [94]. Others might disagree [95].

As such, the hacking of a medical BCI so that it provides additional enhancement not only creates moral concerns, but might also be physically and mentally dangerous for the user herself, and a danger to those around her. As such it is possible that the field of cyberneurosecurity would promote the disincentivization of such hacking to a similar degree that it is not in favor of third-party malicious hacking.

The particular concerns of enhancement via BCIs relate to things like safety and social justice. In terms of social justice, it is likely that availability of BCI technologies and the opportunities to hack them for enhancement will be limited to a small select few with both the skill set, as well as the purchasing power and access to these technologies.

BCI devices that are marketed for recreational use are unlikely to fall under any government oversight vis-à-vis safety [96]. However, the government does provide for oversight of medical devices, and ought to have the ability to prevent those devices from being tampered with unsafely for enhancement purposes. This is especially concerning when medical devices have been tested for limited use, but those who employ those devices for enhancement and recreation are more likely to use the devices more often than they have been clinically trialed for [97], potentially resulting in unforeseen health concerns [98].

11 Countermeasures

The emerging cyberbiosecurity field has also worked to describe and develop putative countermeasures that might begin to deal with some of the concerns raised by this chapter. These include the incorporation of firewalls, antivirus software, whitelists, and blacklists to keep malicious attackers off a BCI's network, cryptographic mechanisms, periodic firmware updates, and even AI technologies that can detect and thwart new and novel attacks. Additionally, some have called for broad use of BCI anonymizer tools that strip all identifying information from BCI data [99]. Regardless of the nature of these countermeasures, practitioners need to develop tools to stress-test and assess the cyber-readiness of various BCIs, especially the increasing number of healthcare devices that employ AI that could obscure or magnify harmful hacks due in part to the lack of transparency and explainability of AI systems [100–102].

The implementations of these countermeasures are non-trivial to implement. Given the aforementioned reference to dancing pigs, security professionals always presume that consumers, including consumers of BCIs, would prefer irrelevant even cosmetic upgrades to their BCIs rather than an upgrade that focused on the security of their devices.

As such, there is a possibility that users who are competent could simply refuse to implement any of these countermeasures and they could not legally be required to upgrade the security of their devices. However, there is also a private law solution: those users could be contractually required to secure their devices with the penalty for failing to upgrade security being the loss of usability of the device. There is precedent with numerous consumer devices wherein the device loses much if not all of their usability if and when the user fails to follow the terms and conditions associated with the use of the device, including the necessary upgrades.

In addition to technological solutions, standards ought to be set that enforce privacy by design [103] and ethical by design [104] products at the manufacturing level [105].

12 Conclusions

We have described herein various aspects of the emerging field of cyberneurosecurity, a subfield of the nearly equally novel field of cyberbiosecurity which is similar but somewhat distinct from the older field of neurosecurity. The further analysis and elucidation of this field are necessary as the state of the art in neuroscience in general and BCIs in particular is advancing quickly. The issues that arise in the field of cyberneurosecurity are also particularly pertinent as they can affect both the general public in addition to the actual user of the BCI, who not only is at risk for physical and mental harm, but could see her emerging neurorights significantly impinged upon. Fortunately, there are many available technological solutions that can be implemented relatively quickly. Unfortunately, there is little overlap between the many different medical and non-medical sectors that employ BCI technology, making it unlikely that we will see broad enforcement, either by government or by the industry itself. Further elucidation of this field will, however, help in promoting necessary oversight as well as additional research into protecting the public.FundingNo industry funding is disclosed.

References

1. Murch R. Security vulnerabilities in the bioeconomy existed prior to synthetic biology. In: Presentation to the NAS National Materials and Manufacturing Board May 1, 2019. https://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_192712.pdf.

2. Potter L, Ayala O, Palmer X-L. Biocybersecurity: a converging threat as an auxiliary to war. In: ICCWS 2021 16th international conference on cyber warfare and security, 2021 p. 291. Academic Conferences Limited.
3. Loohuis K. Dutch researchers build security software to mimic human immune system, May 24, 2021. ComputerWeekly.com.
4. Rauf U. A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions. Arab J Sci Eng. 2018;43(12):6693–708.
5. Pourmoafi S, Vidalis S.. Bio-cyber operations inspired by the human immune system. In: European conference on cyber warfare and security, 2021 (pp. 534–14). Academic Conferences International Limited.
6. Peccoud J, et al. Cyberbiosecurity: from naive trust to risk awareness. Trends Biotechnol. 2018;36:4–7.
7. Puzis R, Farbiash D, Brodt O, Elovici Y, Greenbaum D. Increased cyber-biosecurity for DNA synthesis. Nat Biotechnol. 2020;38(12):1379–81.
8. Randall SM, et al. Cyberbiosecurity: an emerging new discipline to help safeguard the bio-economy. Front Bioeng Biotechnol. 2018;6:39. https://doi.org/10.3389/fbioe.2018.00039.
9. Farah MJ. Neuroethics: the practical and the philosophical. Trends Cogn Sci. 2005;9(1):34–40.
10. Gladden ME. An axiology of information security for futuristic neuroprostheses: upholding human values in the context of technological posthumanization. Front Neurosci. 2017;11:605.
11. Pais-Vieira M, Chiuffa G, Lebedev M, Yadav A, Nicolelis MA. Building an organic computing device with multiple interconnected brains. Sci Rep. 2015;5(1):1–15.
12. Bernal SL, Celdrán AH, Pérez GM, Barros MT, Balasubramaniam S. Security in brain–computer interfaces: state-of-the-art, opportunities, and future challenges. ACM Comput Surv (CSUR). 2021;54(1):1–35.
13. Boccia M, Piccardi L, Palermo L, Nemmi F, Sulpizio V, Galati G, Guariglia C. A penny for your thoughts! Patterns of fMRI activity reveal the content and the spatial topography of visual mental images. Hum Brain Mapp. 2015;36(3):945–58.
14. Wenzel CH. Can thoughts be read from the brain? Neuroscience Contra Wittgenstein. Synthese. 2022;200(3):1–19.
15. Willett FR, Avansino DT, Hochberg LR, Henderson JM, Shenoy KV. High-performance brain-to-text communication via handwriting. Nature. 2021;593(7858):249–54.
16. Verma R, Swanson RL, Parker D, Ismail AAO, Shinohara RT, Alappatt JA, Doshi J, et al. Neuroimaging findings in US government personnel with possible exposure to directional phenomena in Havana, Cuba. JAMA. 2019;322(4):336–47.
17. Hack C. Meet 10 companies working on reading your thoughts (and even those of your pets). Forbes June 21, 2020. https://www.forbes.com/sites/cathyhackl/2020/06/21/meet-10-companies-working-on-reading-your-thoughts-and-even-those-of-your-pets/?sh=4e4c92ab427c.
18. Ienca M, Haselager P. Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics Inf Technol. 2016;18(2):117–29.
19. Ienca and Haselager, supra note 19.
20. Vidal JJ. Toward direct brain–computer communication. Annu Rev Biophys Bioeng. 1973;2(1):157–80.
21. Khan AA, Laghari AA, Shaikh AA, Dootio MA, Estrela VV, Lopes RT. A blockchain security module for brain–computer interface (BCI) with multimedia life cycle framework (MLCF). Neurosci Inform. 2021;2:100030.
22. Bernal G, Montgomery SM, Maes P. Brain–computer interfaces, open-source, and democratizing the future of augmented consciousness. Front Comput Sci. 2021;3:23.
23. Sambana B, Mishra P. A survey on brain–computer interaction. 2022. https://arxiv.org/abs/2201.00997.
24. Bonaci T, Calo R, Chizeck HJ. App stores for the brain: privacy and security in brain–computer interfaces. In: 2014 IEEE International symposium on ethics in science, technology and engineering. Pittsburgh: IEEE; 2014. p. 1–7.

25. Paszkiel S. Using BCI and VR technology in neurogaming. In: Analysis and classification of EEG signals for brain–computer interfaces. Cham: Springer; 2020. p. 93–9.
26. Pal D, Palit S, Dey A. Brain computer interface: a review. In: Computational advancement in communication, circuits and systems. Singapore: Springer; 2022. p. 25–35.
27. Zhang S, Sun L, Mao X, Hu C, Liu P. Review on EEG-based authentication technology. Comput Intell Neurosci. 2021;2021:5229576.
28. Denning T, Matsuoka Y, Kohno T. Neurosecurity: security and privacy for neural devices. Neurosurg Focus. 2009;27(1):E7.
29. Anderson BB, Kirwan CB, Jenkins JL, Eargle D, Howard S, Vance A. How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, pp. 2883–2892. 2015.
30. Vance A, Jenkins JL, Anderson BB, Bjornn DK, Kirwan CB. Tuning out security warnings: a longitudinal examination of habituation through fMRI, eye tracking, and field experiments. MIS Q. 2018;42(2):355–80.
31. Yonas G. NS2 NeuroScience for national security. In: Presented at the end of the beginning—improving warfighter information intake under stress (DARPA augmented cognition mission accomplished Meeting) January 25, 2007. https://www.osti.gov/servlets/purl/1724532.
32. Martinovic I, Davies D, Frank M, Perito D, Ros T, Song D. On the feasibility of side-channel attacks with brain–computer interfaces. In: 21st {USENIX} security symposium ({USENIX} security 12), pp. 143–158. 2012.
33. Markosian C, Taruvai VS, Mammis A. Neuromodulatory hacking: a review of the technology and security risks of spinal cord stimulation. Acta Neurochir. 2020;162(12):3213–9.
34. Pycroft L, Boccard SG, Owen SL, Stein JF, Fitzgerald JJ, Green AL, Aziz TZ. Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg. 2016;92:454–62.
35. Cusack B, Sundararajan K, Khaleghparast R. Neurosecurity for brainware devices. Perth: Edith Cowan University; 2017.
36. Lange J, Massart C, Mouraux A, Standaert FX. Side-channel attacks against the human brain: the PIN code case study. In: International workshop on constructive side-channel analysis and secure design. Cham: Springer; 2017. p. 171–89.
37. Belkacem AN, Jamil N, Palmer JA, Ouhbi S, Chen C. Brain computer interfaces for improving the quality of life of older adults and elderly patients. Front Neurosci. 2020;14:692.
38. Greenbaum D. Ethical, legal and social concerns relating to exoskeletons. ACM SIGCAS Comput Soc. 2016;45(3):234–9.
39. Greenbaum D, Cabrera LY. ELSI in human enhancement: what distinguishes it from therapy? Front Genet. 2020;11:618.
40. Keskin C, et al. Changing an application state using neurological data. US Patent 9, 864,431. 2018 Jan 9.
41. Yuste R, Goering S, Bi G, Carmena JM, Carter A, Fins JJ, Friesen P, Gallant J, Huggins JE, Illes J, Kellmeyer P. Four ethical priorities for neurotechnologies and AI. Nature. 2017;551(7679):159–63.
42. Strickland E, Gallucci M. First win for the Neurorights campaign: Chile plans to regulate all neurotech and ban the sale of brain data. IEEE Spectr. 2022;59(1):26–58.
43. Sententia W. Neuroethical considerations: cognitive liberty and converging technologies for improving human cognition. Ann N Y Acad Sci. 2004;1013(1):221–8.
44. Bublitz J-C. My mind is mine!? Cognitive liberty as a legal concept. In: Cognitive enhancement. Dordrecht: Springer; 2013. p. 233–64.
45. Ienca M, Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. Life Sci Soc Policy. 2017;13(1):1–27.
46. Dadia T, Greenbaum D. Neuralink: the ethical 'Rithmatic of reading and writing' to the brain. AJOB Neurosci. 2019;10(4):187–9.
47. Shemma A, Meirom R, Greenbaum D. The impact of the humanities in science and technology research: a multidisciplinary approach to the ethical, social, and legal impacts of science and innovation. Am J Bioeth. 2016;14(4):20–8.
48. Is this a fact? There's no citation for this, and it seems like a generalization.

49. Zhu G, Huang Y, Wang X. Basic theory of EEG. In: Multi-modal EEG monitoring of severely neurologically ill patients. Singapore: Springer; 2022. p. 3–25.
50. Greenberg J, et al. Privacy and the connected mind—understanding the data flows and privacy risks of brain–computer interfaces. https://fpf.org/wp-content/uploads/2021/11/FPF-BCI-Report-Final.pdf.
51. Greenbaum D. Cyberbiosecurity: an emerging field that has ethical implications for clinical neuroscience. Camb Q Healthc Ethics. 2021;30(4):662–8.
52. Greenbaum D. Avoiding regulation in the medical internet of things. In: Cohen IG, editor. Big data, health law, and bioethics. Cambridge: Cambridge University Press; 2018.
53. Schneier B. Security in the real world: how to evaluate security technology. Comput Secur J. 1999;15:1–14.
54. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care. 2021;33(1):mzaa117.
55. Liu J, Lee HJ, Weitz AJ, Fang Z, Lin P, Choy M, Fisher R, et al. Frequency-selective control of cortical and subcortical networks by central thalamus. elife. 2015;4:e09215.
56. Bernal SL, Celdrán AH, Pérez GM. Eight reasons why cybersecurity on novel generations of brain–computer interfaces must be prioritized. 2021. https://arxiv.org/abs/2106.04968.
57. Sherman M, Idan Z, Greenbaum D. Who watches the step-watchers: the ups and downs of turning anecdotal citizen science into actionable clinical data. Am J Bioeth. 2019;19(8):44–6.
58. Greenbaum D. Avoiding regulation in the medical internet of things. In: Cohen IG, Lynch HF, Vayena E, Gasser U, editors. Big data, health law, and bioethics. Cambridge: Cambridge University Press; 2018.
59. Hildt E. Affective brain–computer music interfaces—drivers and implications. Front Hum Neurosci. 2021;15:711407. https://doi.org/10.3389/fnhum.2021.711407/full.
60. Solterbeck A. Protecting data at rest and in motion. Netw Secur. 2006;2006(9):14–7.
61. Frank M, Hwu T, Jain S, Knight RT, Martinovic I, Mittal P, Perito D, Sluganovic I, Song D. Using EEG-based BCI devices to subliminally probe for private information. In: Proceedings of the 2017 on workshop on privacy in the electronic society, pp. 133–136. 2017.
62. Bernal SL, Celdrán AH, Maimó LF, Barros MT, Balasubramaniam S, Pérez GM. Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. IEEE Access. 2020;8:152204–22.
63. Parastarfeizabadi M, Kouzani AZ. Advances in closed-loop deep brain stimulation devices. J Neuroeng Rehabil. 2017;14(1):1–20.
64. Marin E, Singelée D, Yang B, Volski V, Vandenbosch GA, Nuttin B, Preneel B. Securing wireless neurostimulators. In: Proceedings of the eighth ACM conference on data and application security and privacy, pp. 287–298. 2018.
65. Polania R, Nitsche MA, Ruff CC. Studying and modifying brain function with non-invasive brain stimulation. Nat Neurosci. 2018;21(2):174–87.
66. Landau O, Puzis R, Nissim N. Mind your mind: EEG-based brain–computer interfaces and their security in cyber space. ACM Comput Surv (CSUR). 2020;53(1):1–38.
67. Bonaci T, Calo R, Chizeck HJ. App stores for the brain: privacy and security in brain–computer interfaces. In: In 2014 IEEE international symposium on ethics in science, technology and engineering. Pittsburgh: IEEE; 2014. p. 1–7.
68. Shen G, Horikawa T, Majima K, Kamitani Y. Deep image reconstruction from human brain activity. PLoS Comput Biol. 2019;15(1):e1006633.
69. VanRullen R, Reddy L. Reconstructing faces from fMRI patterns using deep generative neural networks. Commun Biol. 2019;2(1):1–10.
70. Burr C, Cristianini N. Can machines read our minds? Mind Mach. 2019;29(3):461–94.
71. Ren Z, Li J, Xue X, Li X, Yang F, Jiao Z, Gao X. Reconstructing seen image from brain activity by visually-guided cognitive representation and adversarial learning. NeuroImage. 2021;228:117602.
72. Huang W, Yan H, Wang C, Yang X, Li J, Zuo Z, Zhang J, Chen H. Deep natural image reconstruction from human brain activity based on conditional progressively growing generative adversarial networks. Neurosci Bull. 2021;37(3):369–79.

73. Li Q, Ding D, Conti M. Brain–computer interface applications: security and privacy challenges. In: 2015 IEEE conference on communications and network security (CNS). Pittsburgh: IEEE; 2015. p. 663–6.
74. Canham M, Sawyer BD. Neurosecurity. Am Intell J. 2019;36(2):40–7.
75. Patel K, Shah H, Dcosta M, Shastri D. Evaluating NeuroSky's single-channel EEG sensor for drowsiness detection. In: International conference on human–computer interaction. Cham: Springer; 2017. p. 243–50.
76. http://www.smartcaptech.com.
77. Kılıç B, Aydın S. Classification of contrasting discrete emotional states indicated by EEG based graph theoretical network measures. Neuroinformatics. 2022;20:863–77.
78. https://www.technologyreview.com/2018/04/30/143155/with-brain-scanning-hats-china-signals-it-has-no-interest-in-workers-privacy/.
79. LaRocco J, Le MD, Paeng DG. A systemic review of available low-cost EEG headsets used for drowsiness detection. Front Neuroinform. 2020;14:42.
80. https://www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html.
81. Krausová A. Legal aspects of brain–computer interfaces. Masaryk Univ J Law Technol. 2014;8:199–208.
82. https://hbr.org/2019/01/neuromarketing-what-you-need-to-know.
83. Matthews S, Bernal SL, Celdrán AH, Pérez GM. What is it and is it a threat to privacy? In: Clausen J, Levy N, editors. Handbook of neuroethics; 2015. p. 1627–45. https://doi.org/10.1007/978-94-007-4707-4_154.
84. Martinovic I, Davies D, Frank M, Perito D, Ros T, Song D. On the feasibility of side-channel attacks with brain–computer interfaces. USENIX Secur. 2012;12:143–58.
85. Takabi H, Bhalotiya A, Alohaly M. Brain computer interface (BCI) applications: privacy threats and countermeasures. In: IEEE 2nd international conference on collaboration and internet computing. Pittsburgh: IEEE; 2016. p. 102–11.
86. https://openbci.com.
87. https://www.tobii.com/.
88. https://www.roadtovr.com/valve-openbci-immersive-vr-games/.
89. Heller B. Human Rights and Immersive Technology, Carr Center for human rights policy. Cambridge: Harvard Kennedy School; 2020.
90. Heller B. Watching androids dream of electric sheep: immersive technology, biometric psychography, and the law. Vanderbilt J Entertainment Technol Law. 2020;23:1.
91. Mane R, Chouhan T, Guan C. BCI for stroke rehabilitation: motor and beyond. J Neural Eng. 2020;17(4):041001.
92. Buch ER, Santarnecchi E, Antal A, Born J, Celnik PA, Classen J, Gerloff C, et al. Effects of tDCS on motor learning and memory formation: a consensus and critical position paper. Clin Neurophysiol. 2017;128(4):589–603.
93. Parens E. Enhancing human traits: ethical and social implications. Washington, DC: Georgetown University Press; 2000.
94. Erler A. Does memory modification threaten our authenticity? Neuroethics. 2011;4(3):235–49.
95. Coin A, Dubljević V. The authenticity of machine-augmented human intelligence: therapy, enhancement, and the extended mind. Neuroethics. 2021;14(2):283–90.
96. Wexler A. A pragmatic analysis of the regulation of consumer transcranial direct current stimulation (TDCS) devices in the United States. J Law Biosci. 2016;2(3):669–96.
97. Wexler A. Who uses direct-to-consumer brain stimulation products, and why? A study of home users of tDCS devices. J Cogn Enhancement. 2018;2(1):114–34.
98. Goering S, Klein E, Specker Sullivan L, Wexler A, Agüera y Arcas B, Bi G, Carmena JM, et al. Recommendations for responsible development and application of neurotechnologies. Neuroethics. 2021;14(3):365–86.
99. Chizeck H, Bonaci T. Brain–computer interface anonymizer. US Patent App. 14/174818. 2014 Aug 14. http://www.google.com/patents/US20140228701.

100. Zhang X, Ma Z, Zheng H, Li T, Chen K, Wang X, Liu C, Xu L, Wu X, Lin D, Lin H. The combination of brain–computer interfaces and artificial intelligence: applications and challenges. Ann Transl Med. 2020;8(11):712.
101. Olsen S, Zhang J, Liang KF, Lam M, Riaz U, Kao JC. An artificial intelligence that increases simulated brain–computer interface performance. J Neural Eng. 2021;18(4):046053.
102. Aggarwal S, Chugh N. Review of machine learning techniques for EEG based brain computer interface. Arch Comput Methods Eng. 2022;29:3001–20.
103. Cavoukian A. Privacy by design: the 7 foundational principles. Inf Priv Commiss Ontario Can. 2009;5:12.
104. Mulvenna M, Boger J, Bond R. Ethical by design: a manifesto. In: Proceedings of the European conference on cognitive ergonomics 2017. Umea: ITWIL; 2017. p. 51–4.
105. Neuralink. 2023. https://neuralink.com/.