Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity

Article *in* Ethics and Information Technology · June 2016

DOI: 10.1007/s10676-016-9398-9

2 authors:

Marcello Ienca
Swiss Federal Institute of Technology in Lausanne
156 PUBLICATIONS **10,215** CITATIONS

SEE PROFILE

Pim Haselager
Radboud University
136 PUBLICATIONS **3,453** CITATIONS

SEE PROFILE

Ethics Inf Technol
DOI 10.1007/s10676-016-9398-9

ORIGINAL PAPER

Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity

Marcello Ienca[1] · **Pim Haselager**[2]

Abstract Brain–computer interfacing technologies are used as assistive technologies for patients as well as healthy subjects to control devices solely by brain activity. Yet the risks associated with the misuse of these technologies remain largely unexplored. Recent findings have shown that BCIs are potentially vulnerable to cybercriminality. This opens the prospect of "neurocrime": extending the range of computer-crime to neural devices. This paper explores a type of neurocrime that we call *brain-hacking* as it aims at the illicit access to and manipulation of neural information and computation. As neural computation underlies cognition, behavior and our self-determination as persons, a careful analysis of the emerging risks of malicious brain-hacking is paramount, and ethical safeguards against these risks should be considered early in design and regulation. This contribution is aimed at raising awareness of the emerging risk of malicious brain-hacking and takes a first step in developing an ethical and legal reflection on those risks.

Keywords Brain–computer interfacing · Neurosecurity · Privacy · Neurocrime · Brain-hacking · Autonomy · Agency

✉ Marcello Ienca
marcello.ienca@unibas.ch

Pim Haselager
w.haselager@donders.ru.nl

[1] Institute for Biomedical Ethics, University of Basel, Bernoullistrasse 28, 4056 Basel, Switzerland

[2] Donders Institute for Brain, Cognition and Behaviour, Radboud University Nijmegen, B.01.13 Spinoza Building, Montessorilaan 3, 6525 HR Nijmegen, The Netherlands

Published online: 16 April 2016

It is always too early to assess a technology, until suddenly it is too late.
Martin Buxton (Buxton 1987).

Introduction

The term brain-hacking refers to the emerging possibility of coopting brain–computer interfaces (BCI) and other neural engineering devices with the purpose of accessing or manipulating neural information from the brain of users. This paper offers an overview of the possible sorts of brain-hacking to which BCIs are or may become subject in the near future and provides an inventory of the specific ethical implications of brain-hacking. We will proceed as follows: first, we will discuss the main features of computer crime. Second, we will discuss the main features of neurocrime and brain-hacking. Third, we will offer a brief description of the BCI cycle. Fourth, we will identify what specific types of brain-hacking can occur at each phase of the cycle. Finally, we will delineate the major ethical implications emerging out of the phenomenon of brain-hacking. Although the ethical concerns we discuss in relation to brain-hacking may be found in relation to other technologies as well, we suggest that their particular combination with respect to BCI warrants a separate discussion, especially given the current and to be expected progress in BCI research and applications. Therefore, our aim is to provide a systematic treatment of the various ways of brain-hacking in relation to the different components of BCI. This contribution is aimed at promoting a public debate over the potential threats to neurosecurity related to the potentially widespread availability of BCIs among the general public, and takes a first step in developing a systematic ethical and legal reflection on brain-hacking. Future research is required to extend this analysis and to develop a comprehensive ethical, legal and regulatory framework.

Computer crime

The number and quality of human activities enabled or mediated by computers is increasing rapidly. Emerging trends in information and computer technology such as big data, ubiquitous computing, and the Internet of Things are accelerating the expansion of computer use in our societies. Today, computers are used to perform or facilitate an enormous variety of tasks and activities of daily living including, but not restricted to, banking, trading, scheduling and organizing events, learning, entertaining, gaming and communicating. Computer use does not restrict solely to the social and economic domain. Several activities that are considered inherent to our psychological and biological dimension are now supported or facilitated by computing. Examples include the use of GPS systems in geolocation and spatial navigation, the use of wearables in monitoring bodily processes such as calories intake, heart beat rate, and weight loss, and the use of personal computers in performing cognitive tasks such as arithmetic calculus, writing, and memory.

As the uses of computers in human life have increased both in volume and in richness, the security threats to computing have also increased significantly. Notoriously, computer and information technologies can be used by actors for nefarious purposes such as cracking, fraud, identity theft, financial theft, and information warfare. The broad range of criminal activities that result from misusing computers and networks is referred to as *cybercrime*. Halder and Jaishankar (2011) define cybercrime as: "Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks" (Halder and Jaishankar 2011). Originally, cybercriminal activities were restricted to personal computers and related computer networks. With the dramatic expansion of the digital ecosystem many new opportunities for malicious exploitation should be expected. It is predicted that the current number of devices connected to the Internet will increase from 9 billion in 2011 to 50 billion in 2020, generating a flow of 50 trillion GBs of data (Evans 2011). Devices such as watches, TVs, eye-wears, home-appliances, automobiles and medical devices are increasingly becoming sources of computational information and will irrigate the digital ecosystem with an unprecedented quantity of data flows and at an unprecedented velocity. This will also multiply the quantity of data and the number and type of devices that are potentially exposed to cybercriminality.

Many of the technologies responsible for this dramatic expansion of the digital ecosystem fit in the category of *disruptive technologies* as they make a lasting change to the technological landscape. Although disruptive technologies are designed to positively impact individuals and society, their technological novelty also opens 'breaches' for criminals. These breaches, as Dupont points out, are often "the result of a defective legal or regulatory coverage and provoke rapid increases in offenses" (Dupont 2013). In fact, regulation upgrade occurs at a much slower rate than technology upgrade and present security regulations are often incapable to effectively account for the accelerating changes generated by technology in human activities and infrastructures.

In this rapidly changing context, the goals of computer security, namely the protection of the confidentiality, integrity, and availability of information become more difficult to achieve (Denning et al. 2009). This increased difficulty does not arise exclusively from the quantity and velocity of data. Rather, the quality of information introduced into the data flow is crucial too. The more pervasive computing technology becomes, the more intricately it is interwoven into the everyday life. While this has the significant benefit of minimizing interaction friction between humans and machines, hence making computer-use effortless and more personalized, it also multiplies the classes of information that become accessible, hence potentially exposed to cybercriminal risks. Among these classes of information, biological information is critical.[1] Medical computer technologies such as artificial cardiac pacemakers as well consumer-grade technologies such as wearable heart rate monitors are designed with the purpose of accessing and processing biological information –in this case, information about the beating of the heart. As the use of bioengineering devices is rapidly increasing, the amount of biological information irrigating the digital ecosystem will increase as a consequence. This raises the issue of privacy and information security, as biological information is carrier of private and sensitive data whose access or manipulation by malicious actors may cause significant physical (including life-threatening), psychological or social harm to technology users. An example of this emerging risk was provided by Halperin et al. (2008) who experimentally demonstrated that a hacker could wirelessly compromise the security and privacy of an already commercialized implantable cardiac defibrillator. In their

[1] The notion of biological information is used in this paper to extensively refer to information expressed in the processes characteristic of living organisms at various levels, i.e. at the levels of molecules, cells, organs, circuits etc. This definition is in accordance with the statistical definition of information formulated by Claude Shannon and used in mathematical information theory (Shannon 1949). In Shannon's sense, "anything is a *source* of information if it has a range of possible states, and one variable *carries* information about another to the extent that their states are physically correlated". For a comprehensive understanding of the notion of biological information see: (Godfrey-Smith and Sterelny 2007).

experiment, hackers could use homemade and low-cost equipment to change a patient's therapies, disable therapies altogether, and induce potentially fatal processes such as ventricular fibrillation (Halperin et al. 2008).

Neurocrime

The problems of technology misuse and security of biological information are particularly critical in the context of neurotechnology as this type of technology applies (either directly or indirectly) to a very important organ in the human body, the brain. The brain not only contributes significantly to life-maintaining processes (such as nutrition and respiration) but also to faculties such as consciousness, perception, thinking, judgment, memory and language and is of great importance to our behavior and our self-identification as sentient-beings or persons. Therefore, misusing neural devices for cybercriminal purposes may not only threaten the physical security of the users but also influence their behavior and alter their self-identification as persons. We call the realm of cybercriminal activities enabled by the misuse of neural devices *neurocrime*.

It is worth noting that neurocrime does not necessarily involve direct access to the brain and to brain information. Rather, neurocriminal activities are most likely to occur, at present, in a manner that affects the brain only indirectly, for example by limiting, modifying or disrupting function in the devices that interface brain computation. This type of risk is already critical at the current level of deployment of neural engineering technologies. With neurally controlled devices (e.g. brain stimulators and brain–computer interfaces) being available as medical technologies as well as commercialized products, present neurocriminals may abuse of the users by disrupting or terminating function in their devices without the users' permission or consent. For example, neurally controlled robotic limbs used to compensate for the motor deficits of amputated patients are potentially vulnerable to being mechanically destroyed by malicious actors, which would deprive the users of their re-acquired motor abilities. This type of neurocrime affects the brain only indirectly since the users' neural computation is not directly accessed or manipulated in any significant sense during the attack. Nonetheless, criminal activities of this type may affect significantly the mental life of the victims, because these activities can limit and constrain their behavior, generate emotional responses such as panic, fear, and psychological distress, and leave traumatic memories. In the light of this and in accordance with the previously reported definition of computer crime, we define the emerging phenomenon of neurocrime as offenses against individuals or groups of individuals with a criminal motive to intentionally cause direct or indirect physical and mental harm to the victim as well as harm to the victim's reputation and property by accessing or manipulating neural information through the use of neural devices. It is worth noting that, under some circumstances, the attacker and the target of the attack may be the same person. For example, mentally unstable users of prosthetic limbs may choose to damage their devices in an attempt to perform self-imposed harm.

From the perspective of neurocrime two types of neural devices are particularly critical at present: brain stimulators—especially deep brain stimulation (DBS) and transcranial direct-current stimulators (tDCS)[2]—on the one hand, and brain–computer interfaces (BCIs) on the other hand. The reason for that stems from three basic facts common to both types of neural device: (1) they potentially enable direct access to neural computation, although in diametrically opposite ways—brain stimulation versus reading of brain activity; (2) their use is widespread as they are both available not exclusively as medical technologies but also as commercialized products for healthy users (3) they have the potential to generate safety and security concerns.[3] Being the only type of neural devices whose hackability has been proven in experimental and real-life settings, BCIs will be the only neural technology at stake in this paper. Further research is required to explore the specific neurocriminal risks associated with DBS, tDCS and other forms of neurostimulation.

Brain–computer interfacing

In contrast to neurostimulators, brain–computer interfaces are not used to stimulate the brain but establish a direct communication pathway that allows BCI-users to control an external computer device exclusively with brain activity, bypassing the peripheral nervous and muscle systems (Vallabhaneni et al. 2005). BCIs originally developed in

[2] Deep brain stimulation (DBS) is an invasive neurostimulation technique which involves the neurosurgical implantation of a medical device into the brain. This implanted device sends electrical signals into targeted subcortical areas with the aim of eliciting activity. DBS is an increasingly used therapy for several neurological conditions such as Parkinson's disease, dystonias, essential tremor, and chronic pain syndromes when patients are not responding to less invasive approaches (Tronnier and Rasche 2015).

Transcranial direct current stimulation is a neuromodulatory intervention which uses constant, low electrical current delivered to the cortical area of interest via small electrodes placed on the skull with the aim of changing neuronal excitability in that area (Brunoni et al. 2012). This change of neuronal excitability may influence, and in certain cases enhance cognitive performance for a brief period of time on a number of different cognitive tasks.

[3] See, for example, the following two magazine reviews: (Conner 2010; Strickland 2014). Although concerns expressed by popular media may at times be exaggerated, they still may require appropriate responses by scientists and ethicists, if only to diminish or forestall unrealistic worries amongst the general public.

clinical medicine as a therapeutic or assistive technology for neurological patients. In clinical settings, BCI-applications are directed at repairing, assisting or augmenting cognitive or sensory-motor functions in patients experiencing cognitive or sensory-motor impairments including spinal cord injury, stroke, and motor neuron disease such as amyotrophic lateral sclerosis (ALS) and muscular dystrophy (Allison et al. 2007; Vallabhaneni et al. 2005). For example, BCI-based motor prostheses have successfully been trialed in animal models and patients to enable direct brain control on artificial limbs, wheelchairs and other devices (Fetz 2015). To date, BCI-applications are available not only within clinical settings but also to the general public. Several commercial applications of EEG-based BCI devices have made their way onto the market and are becoming increasingly popular among healthy individuals for gaming and supporting everyday activities. For example, companies *Emotiv* (http://emotiv.com/) and *Neurosky* (http://www.neurosky.com) have pioneered the commercialization of consumer-grade non-invasive and easy-to-wear BCIs for gaming, interactive television, or as hands-free control systems. The electronic telecommunication industry is providing consumer-grade BCIs that are available for potential mass adoption. For instance, iPhone accessories such as Xwave© allow the headset to plug directly into compliant iPhones and read brainwaves. Meanwhile, prototypes of next-generation Samsung Galaxy Tabs and other mobile or wearable devices have being tested to be controlled by brain activity via EEG-based BCI (Powell et al. 2013). In addition, neuromarketing companies such as Nielsen (http://www.nielsen.com/) are using BCI-applications to better assess customer needs and preferences.[4] Given the significant potential benefits of brain control in computing—e.g. immediacy, hands-free control, portability etc.—Yuan and colleagues predict that BCIs will gradually replace the keyboard, the touch screen, the mouse and the voice command device as humans' preferred ways to interact with computers (Yuan et al. 2010). Finally, a number of military and warfare BCI-applications are currently in development. The US Defense Advanced Research Projects Agency (DARPA) is currently funding a broad spectrum of BCI projects with two major purposes: (1) restoring neural and/or behavioral function in warfighters, and (2) enhancing training and performance in warfighters and intelligence agents (Kotchetkov et al. 2010; Miranda et al. 2015). For example, the Neurotechnology for Intelligence Analysts (NIA) has developed BCI systems utilizing non-invasively recorded EEG to significantly increase the efficiency and throughput of imagery analysis (Miranda et al. 2015).

[4] http://www.nielsen.com/us/en.html (last accessed May 3, 2015).

While the potential benefits and predicted distribution of clinical and non-clinical applications of BCI technology are significant, the neurosecurity risks associated with the widespread availability of this technology remain largely unexplored.

From neurocrime to brain-hacking

Denning et al. (2009) provide prototype-examples of neurocrime. These include the wireless hijacking of a prosthetic limb, the malicious re-programming of neurostimulation therapy (e.g. the wireless alteration of the device settings to generate unsafe brain stimulation) and the eavesdropping of a brain implant's signals to reveal private information. These examples describe very specific neurocriminal phenomena where the attack is not simply directed at disrupting the neural device but at getting direct access to brain information. Neurocriminal activities of this type appear more specific than general neurocrime as (1) can only be performed on neural devices that establish a direct connection pathway with the brain such as tDCS, neural implants and BCI, (2) involve the direct access to and manipulation of neural information, (3) influence directly neural computation in the users. We call this special type of neurocrime malicious "brain-hacking" as it exploits the neural device to get illicit access to and eventually manipulate brain information in a manner that resembles how computers are hacked in computer crime. As in general neurocrime, also in brain-hacking the attacker and the target of the attack may be the same person. For example, a user may hack his or her own neurostimulation device to self-prescribe elevated moods or increase activation of reward centers in his or her brain (Denning et al. 2009).

Li et al. (2015) have provided an inventory of possible malicious brain-hacking activities based on the type of BCI application. They distinguish four types of BCI applications: (1) neuromedical applications, (2) user authentication, (3) gaming and entertainment, and (4) smartphone-based application (Li et al. 2015). For each of these application families they presented the current attack scenario and suggested possible countermeasures. Some forms of brain-hacking have already proven to be actually feasible in experimental as well as in real-life settings. Rosenfeld et al. (2006) have shown that brain–computer interfaces can be coopted to detect concealed autobiographical information from users with a significantly high accuracy rate (Rosenfeld 2011). More strikingly, Martinovic et al. (2012) have successfully used brain–computer interfaces to reveal private and sensitive information about the users such as their pin codes, bank membership, months of birth, debit card numbers, home location and faces of known persons (Martinovic et al. 2012). We will discuss these possibilities in more detail below in the "Input manipulation" section.

A sci-fi future where people can access and manipulate information in other people's brains is approaching and their prodromes are already here. Therefore, unless appropriate safeguards are considered early in the design of the neural devices that will be deployed in the next future (5–20 years), concerns of malicious misuse in the form of brain-hacking could become paramount for public safety.

The BCI cycle

BCIs can be distinguished into two types: invasive and non-invasive. Invasive BCIs record brain signaling via surgical implantation of electrode arrays in or directly connected to the central nervous system. Non-invasive BCIs interface brain signaling via neuroimaging technologies such as electroencephalography (EEG) and electromyography (EMG) that record brain activity through electrodes placed on the outside of the skull. As said previously, both invasive and non-invasive BCIs establish a direct interaction between the user's brain and a computer device. This interaction is usually described as a 4-phase cycle (van Gerven et al. 2009). See Fig. 1.

The first phase concerns the input, i.e. the generation of specific brain activity by the user in response to a stimulus. This brain activity is generated when the BCI-user is in a certain cognitive state or performs a mental task. For example, when a BCI user is controlling a wheelchair a matrix of possible itinerary choices is presented on the interface that the user is watching. A frequent brain activation pattern used in BCI are the so-called event-related potentials (ERPs), i.e. measured brain responses that are the direct result of a specific sensory, cognitive, or motor event. Among these ERPs, increasing interest is surrounding the P300 wave, an ERP component usually elicited in the process of decision making (Fazel-Rezai et al. 2012). In our example, when the desired itinerary is presented (e.g. by highlighting or 'flashing' it) at the interface, the user's brain signals will contain a P300 signal that can be picked up by the BCI.

The second phase concerns the measurement and recording of brain activity. At this stage, patterns of brain activity in the user's brain are detected and measured by the interface during a cognitive process or the performance of a mental task. For example, when a certain itinerary option upon which the BCI-user is focusing is flashed (say, a specific end-location, or an instruction to turn left), the BCI can detect the P300 wave elicited at that moment. The measurement can be implemented in several ways according to the type of BCI in use. The most frequent type of BCI is based on electroencephalogram (EEG); other measurement options include magnetoencephalography (MEG), and functional magnetic resonance imaging (fMRI).

In order to be usable for the BCI and generate appropriate outputs (i.e. those expected by the user), the raw data measured in the second phase should be decoded into its main features and classified. This decoding and classifying process typically occurs in the third phase of the BCI cycle. In this phase, data are processed in order to 'clean' the brain signals, namely to increase the signal-to-noise ratio

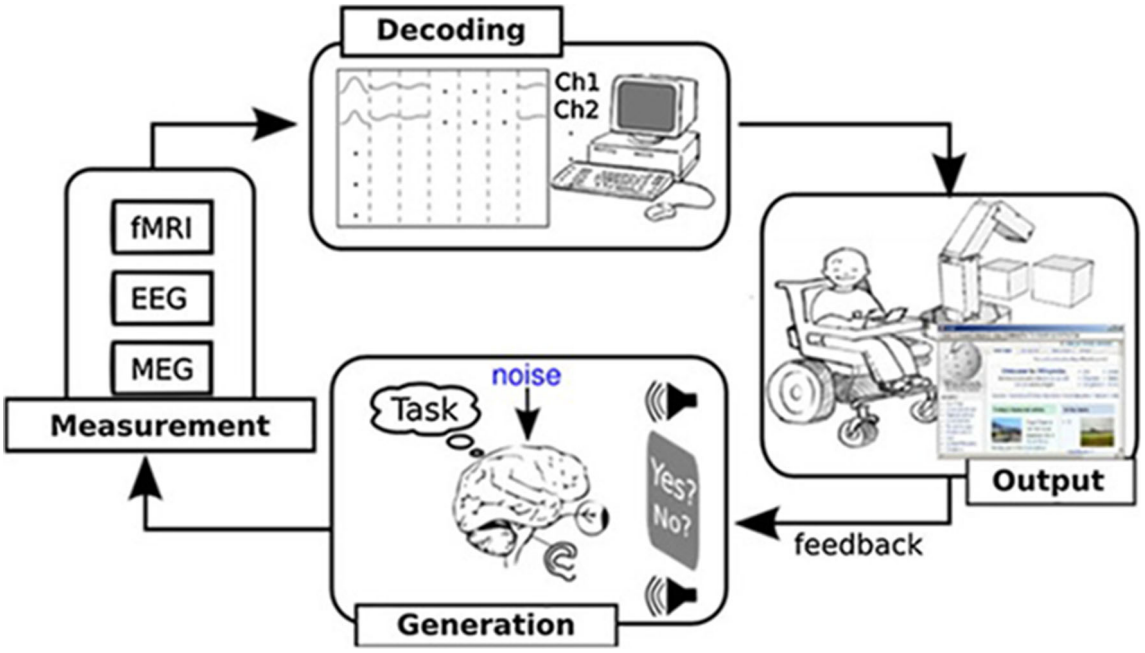

Fig. 1 The BCI cycle *Source*: Figure adopted, with permission, from J. Farquhar/Braingain

(i.e. a measure of strength of the desired signal relative to background noise) and to filter the most relevant aspects of each signal for further processing. This processing is necessary to extract the relevant features from the signal and distinguish them from non-relevant features, especially from the background noise due to the underlying brain activity that is not directed at the execution of that specific mental task (in our example, the activity that is not directed at moving the wheelchair, e.g. processes involved in color perception).

Once the signals are decoded, they can be translated into output. The output is usually the performance of the action initially intended or desired by, or deemed beneficial for, the user through the control of the applications interfaced by the BCI (in our example, turning left with the wheelchair). Controllable applications include motor devices (e.g. wheelchairs and robotic limbs), sensor devices as well as several software and hardware applications (including apps for smartphones). Once each cycle is completed the user can perceive the feedback resulting from the previous cycle (e.g. notices the wheelchair turning left) and the next cycle can start.

Brain-hacking

Brain-hacking can in principle occur at each of the different phases of the BCI-cycle. In the following, we will provide an overview of the sorts of brain-hacking to which BCIs are subject at present or may be subject in the near future according to the phase of the BCI-cycle at which the attacks may occur. For each sort of attack it will discuss the corresponding criminal activities that can be committed and the type of moral values and norms that are at stake.

Input manipulation

Brain-hacking via input manipulation occurs when the hacker attacks the BCI user at the moment of providing input, i.e. at the first phase of the BCI cycle.[5] Input information can be manipulated by altering the stimuli presented to the user. For example, brain-hackers may preselect target stimuli to elicit specific responses in the user that facilitate the access the user's neural information. This type of hack has been proven to be actually feasible by recent research in computer security and human–computer interaction. For example, Rosenfeld et al. (2006) have developed a P300-based protocol to detect concealed autobiographical information from users with a significantly high accuracy rate (Rosenfeld et al. 2006). Van Vliet et al. (2010) have used the N400 component of ERP to detect what a BCI user is 'thinking about' without using explicit stimuli (van Vliet et al. 2010).[6] Particularly striking are the results by Martinovic et al. (2012). In this study, researchers presented EEG BCI-users with six classes of stimuli: (1) PIN code digits, (2) photos related to banks, (3) names of the months, (4) debit card digits, (5) locations, and (6) faces. For each class, one target stimulus (i.e. stimulus eliciting sensitive information known to the user) was inserted in the randomly permuted sequence of non-target stimuli (Martinovic et al. 2012). For example, in the bank experiment, the target stimulus was the picture of an ATM machine from the user's bank whereas the non-target stimuli were a series of pictures of ATMs from other banks. The goal of the study was to detect a P300 signal in response to private and sensitive information about the users (their pin codes, bank membership, month of birth, debit card numbers, home location and faces of known persons) and extract that information. Since this information is usable for monetary transactions, home banking and log-into private on-line accounts, extracting this information may enable hackers to perform offenses against BCI users. The results show that this sort of input-manipulation can turn the BCI against users in order to reveal some private information with a significant chance of success: in fact, the Shannon entropy of the private information was decreased on the average by approximately 15–40 % compared to random guessing attacks[7] (Martinovic et al. 2012, p. 1). Such sorts of malware resemble the function of computer spyware as they aid in gathering information about a user, in sending it to another entity, or in asserting control over a computer or computer-driven device without the user's permission or consent. Unlike common spyware, however, the malware involved in brain-hacking extracts information directly from brain signaling, hence the name 'brain-spyware'. The potential set of applications of brain-spyware in future cybercrime is large and may involve several criminal activities such as password cracking, identity theft, phishing and fraud.

[5] It is worth noting that there are two potential meanings of *input* here: (1) the user provides input to the BCI through brain activity; (2) the interface provides information (e.g. a screen with commands) to the user. To disambiguate, in this section we will refer exclusively to the latter as this type of input is the only one whose hackability was proven in the experimental setting.

[6] The ambiguous term 'thinking about' is defined by the authors as 'being primed on'. Since the priming effect occurs for many types of stimuli (e.g. words, sounds, and images) the authors assumed that a subject can prime himself by being told to think about an object. See van Vliet et al. (2010, p. 183).

[7] In order to quantify the information leak that the BCI attack provides, the researchers compared the Shannon entropies of guessing the correct answers for the classifiers against the entropy of the random guess attack. The entropy difference directly measures the information leaked by an attack; see Martinovic et al. (2012, p. 11).

An additional breach for brain-hacking via input-manipulation is authentication via EEG signal. Li et al. (2015) have reported an attack model by impersonating the thoughts of subjects using EEG generative model based on the historical EEG data from a subject (Li et al. 2015).

It is worth to point out that at the current level of development of BCI technology three major technical limitations prevent the diffusion of brain-hacking cases outside the clinical setting: (1) measurement accuracy, (2) processing speed, and (3) distribution. As we have seen in the previous chapter, in the decoding phase of the BCI cycle data must be processed in order to increase the signal-to-noise ratio and segregate relevant from non-relevant information. For today's hackers, decoding brain signals with a level of accuracy and at a speed comparable to cracking computer codes is still impossible outside the experimental settings. This is exacerbated, by the limited commercial distribution of portable BCI-applications. Given the limited readability of brain signals and the current level of maturity of the market, for today's hackers the reward may not be worth the risk. However, as technology advances and the BCI-market rapidly expands, brain data will reveal more and more and their level of readability will rapidly increase.

Measurement manipulation

Brain-hacking can also occur when the hacker attacks the BCI user during the phase of the measurement in order to generate—without the user's permission—outputs that are different from those expected to be generated by regular processing. Attacks of this type may differ with regard to their purpose. Three main criminal purposes are foreseeable: cracking the BCI's raw data, disrupting BCI's function, and hijacking the BCI. A real-life protoexample of BCI-cracking is the so-called Cody's Emokit project, developed by the hacker Cody Brocious. Brocious cracked the encryption of a consumer-grade BCI produced by Emotiv (called EPOC) and built a decryption routine. Subsequently, he created an open-source library for reading encrypted data directly from the headset, and posted about his project on the Emotiv user forum. As Conner explains: "his library of code hacks to the device just pulls raw data from the unit; there's no ability to filter the signals or tell which sensor corresponds to each data stream" (Conner 2010). It is worth to highlight that Brocious' hack had no malicious motive. In contrast, it was designed to open EPOC's source code and open up the device to development (hence with the ethical purpose of accelerating secure new products and research). However, malevolent agents can use similar strategies to illicitly crack information as a form of dual-use.

Attacks by BCI disruption may occur when the hacker aims at manipulating the measuring process in order to confuse, sabotage or delay the function of the BCI application. The function of a BCI can be disrupted, at the level of measurement, by adding noise to make the measurement inaccurate. Hijacking may occur when the hacker tries to monitor and alter the BCI communication channel with the purpose of diminishing or even replacing the user's control of the BCI application. During hijacking the system is given other commands than those intended or desired by the user, for the benefit of the hacker. Brain-hackers could manipulate the measurement by adding noise in order to diminish or eliminate control of the user over the BCI application. For example, a frustrated caregiver could hijack a BCI-enabled speech production device to silence a cognitively impaired user or a wheelchair to force the user to follow a certain itinerary. More generally, measurement manipulation by hijacking may result in several criminal activities aimed at limiting, harming or taking advantage of the BCI-users' behavior.

Decoding and classifying manipulation

Brain-hacking at the level of decoding and classification is also aimed at generating outputs that are different from those intended or desired by the user, and expected to be generated by regular processing. This criminal goal may be achieved in three ways: (1) by adding noise to simply make the decoding process unduly difficult; (2) by intervening with the machine learning component (so strictly speaking, moving to the feature classification phase) in order to manipulate the classification of the brain signal; or (3) overriding the signal sent by the BCI to the output device.[8] Each of these hacking strategies will have peculiar pros and cons. For example, the noise-adding hack will have the advantages (from the perspective of malicious actors) of being more easily performable and less easily detectable than the other two but it will also make it more difficult for the hackers to have the BCI application do what they want. In contrast, the other two hacking strategies will be more difficult to perform and more easily detectable than the former but they will, in principle, enable the hackers to have more control over the BCI system. Similarly as in measurement-manipulation, brain-hackers can intervene at the level of decoding and classification with the criminal motive of hijacking the BCI-application. The peculiarity of attacks at this phase of the cycle, however, is that the hijacking may not be simply aimed at diminishing or expunging the control of the user over the application, but also at replacing control. Brain-

[8] It is worth noting that the first strategy (adding noise) is similar to the one discussed in "Measurement manipulation" section with regard to measurement manipulation. However, at this level, the consequence we discuss may be different as the aim of the intervention here is to delay or complicate the decoding process.

hackers may try to monitor and alter or inject messages into the BCI communication channel with the purpose of replacing the user's control of the BCI application. During hijacking, the system is given other commands than those intended or desired by the user, for the benefit of the hacker. Successful hijacking will result in the hacker having partial or full control over the BCI application and the BCI user having diminished or no control on the application. This would expose the user to perils directly or indirectly induced by the hijacker. For example, a criminal actor could hijack the BCI-controlled smartphone of a BCI-user without the user's permission to extort payments, erase sensitive information or communicate with third parties by masquerading his or her identity under the identity of the user (hence performing offences including fraud, theft and identity theft). In addition, as we have seen before, hijacking strategies could also become sources of threat to the personal safety of third parties, as the hijacked device could harm third parties either accidentally or as an explicit command of the hijacker.

Although no confirmed real-life or experimental reports of hacking via measurement or decoding and classifying manipulation are available at present, these types of brain-hacking deserve particular monitoring in the context of security, surveillance and public health. The reason for that stems from the fact that their potential nefarious outcomes are not exclusively restricted to actions involving the access to sensitive information (e.g. identity theft and fraud) but extend to more detrimental activities involving the physical and psychological harm of the users.

Feedback manipulation

Brain-hacking by feedback manipulation would occur when the hack is aimed at altering the feedback perceived by the user at the end of each cycle. This type of hack would aim at manipulating the perception that the user has of previous actions performed or the self-perception of previous cognitive states generated through the BCI. The criminal motive underlying these hacks would be to induce—without the user's permission—particular cognitive states or actions in the subsequent cycle of the user for the advantage of the hacker. For example, brain-hackers could perform a sort of "brain-phishing" in which the user is required by the hacker to insert a password or another type of authentication information before the originally intended process can continue (e.g. a user could be asked for a password to actually start the program she has mentally commanded). Through the same mechanism, traumatic experiences could be induced in the user to his or her detriment. Criminal activities performable through this hack may include fraud, phishing, identity theft, and physical or psychological harm.

These different sorts of hack with their related type of malware, and potential criminal activities are presented in Table 1.

Ethical implications

These four sorts of brain-hacking have several ethical and legal implications. Some of these implications are cross-categorical, i.e. apply to all forms of brain-hacking, whereas some others are peculiar to a specific category of hack. In this section an inventory of the ethical implications of brain-hacking will be provided. Further research is required to develop each of these implications into a detailed ethical and legal analysis to inform future regulatory strategies for the prevention of neurocrime.

The dual-use dilemma of brain-hacking

Cross-categorical ethical implications involve the general problem of dual-use and the obtainment of informed consent. By dual use it is meant the fact that the same beneficial scientific knowledge or technology can be used for good as well as for nefarious purposes (Pustovit and Williams 2010). Dual-use is a particularly crucial ethical concern in computer, telecommunication and information technology, since computers and networking technologies are frequently used by actors for cybercriminal purposes. Therefore, the ethical implications of dual-use, in particular the dual-use dilemma, also apply to BCI technology and the phenomenon of brain-hacking.

The peculiar dual-use dilemma of brain-hacking can be summarized as follows: the same neural device (e.g. the same BCI) has the potential to be used for good (e.g. assisting cognitive function in neurological patients) as well as bad purposes (e.g. identity theft, password cracking and other forms of brain-hacking). This dilemma is primarily faced not only by researchers and technology developers, but also by companies because of their potential product liability and by governments as they are committed to promoting health and security of their citizens.

At the current level of diffusion and sophistication of brain-hacking, the benefits produced by BCI development for patients and society significantly overwhelm the risks associated to brain-hacking and other neurocrime. Although some mild forms of brain-hacking have been proven feasible in experimental settings or in real-life tests (as in Cody's Emokit project), there is no confirmed report of criminal and/or detrimental activities involving BCI to date. However, the phenomenon of brain-hacking should be constantly monitored and appropriate safeguards should be considered early in the design and deployment of the

Table 1 Synoptic view of malicious brain-hacking

Phase	Type of attack	Criminal activity	Ethical problem	Proved feasibility
Input	Providing misleading input	Password/PIN cracking	Privacy	√
		Identity theft	Confidentiality	
		Fraud	Personal security	
		Phishing		
Measurement	Noise addition	Disruption	Psychological distress	–
	Manipulating classification	Termination	Physical harm	
		Hijacking	Diminished agency	
Decoding	Overriding signal sent to output	Disruption	Psychological distress	–
		Termination	Physical harm	
		Hijacking		
Output	Feedback alteration	Disruption	Diminished agency	–
		Termination	Psychological distress	
		Hijacking	Physical harm	
			Uncertain personhood	
			Uncertain moral responsibility	

neural devices as the opportunities for criminal offense and malicious exploitation related to BCI are predicted to significantly increase in the near future. These safeguards may include:

- The development of mechanisms and methods for anonymizing neural signals. A promising example of this is the Brain–Computer Interface Anonymizer (patent US 20140228701 A1), a method to generate anonymized neural signals by filtering features to remove privacy-sensitive information (Chizeck and Bonaci 2014).
- The deployment and integration of security mechanisms to detect uncharacteristic increase of noise in BCI-processing at the level of measurement as well as at the level of decoding and classification.
- The deployment of feedback mechanisms for users to allow them to signal clearly undesired or uninitiated output of the device. In vulnerable (e.g. physically disabled or cognitively impaired) users these feedback mechanisms may be connected to alarms and/or location services that allow the hacked-users to automatically alert a response center (e.g. their caregivers or public safety authorities) and receive prompt support.
- The deployment of machine learning self-control mechanism for detecting severe inconsistencies in the classification of features. These self-consistency check mechanisms could detect criminal circumstances where the brain-hack occurs at the level of decoding and classification of features.
- The provision of specific training sessions for clinical BCI-users to train the users' resistance to brain-hacking, especially brain-hacking via input-manipulation. These trainings could include the instruction of specific responses to potentially unsafe stimuli such as those related to banking and authentication methods and could be directly provided by the health-care institution where the user is allocated.
- The inclusion of free neurosecurity demos into the BCI-package for general users. Future commercially available BCI-packages may include a small introduction software package containing a brief serious game demo with instructions and safety-guidelines related to brain-hacking.

It is a major role for current neural engineering and information security organizations to call for awareness regarding the dual-use risks associated with brain–computer interfacing and design regulatory mechanisms that could enhance the safety and security of present and future BCI applications. In addition, it is important to raise awareness among the general public on the ethical implications associated with the phenomenon of brain-hacking and to stimulate the understanding and practical application of guidelines aimed at protecting and promoting the privacy, autonomy and integrity of the individual.

Informed consent

Ethical issues with respect to informed consent for BCI-use interventions especially focus on the ratio between the high expectations that BCI technology may generate and the possible vulnerability of potential BCI users (Clausen

2011). For example, in the case of severe neuromuscular patients such as LIS patients, high expectations on the liberating effect of BCI technology may represent a major ethical challenge, since these expectations could undermine patients' evaluation of risks and benefits, including the risks associated with the phenomenon of brain-hacking. Vulnerable patients may be more likely to accept a higher risk of information insecurity, hence become more exposed to brain-hacking. To prevent this, accurate monitoring and reporting of the phenomenon of brain-hacking is recommended not only for scientists and ethicists but also for technology producers and the media. Inaccurate or insufficient reporting may result in generating unrealistic expectations in patients and reducing their perception of risk. In addition, more rigorous procedures for informed consent should be implemented to increase the user's understanding of the risk–benefit ratio. It is worth remembering that getting informed consent is especially challenging when communicating with severely paralyzed target users such as those suffering LIS. Impaired communicative capacities of LIS patients require paying attention also to some characteristics of information and communication that are not reducible to verbal communication (e.g. eye blinking). As Clausen (2011) note, this is especially important for the questions whether the patient understands the information correctly, and whether there are any questions left for him/her (Clausen 2011).

Privacy, confidentiality and security

Particular ethical problems are posed by each single sort of hacking. Two major ethical problems are associated with hacking through input-manipulation. The first one is privacy. The possibility of extracting private and sensitive information from the brain of users represents a significant treat to privacy and data protection. Users that are victims of this sort of brain-hacking typically lose the ability to seclude confidential or inherently sensitive information about themselves, thus experience an intrusion of their private sphere (Bonaci et al. 2014). This ethical problem is particularly significant because privacy is a priority issue in a free society, closely linked to civil liberties, democracy and human rights (Westby 2004). The protection of privacy and confidential data is a primary commitment in the United States as well as in the European Union where there is a collaborative push for modernizing the current data protection principles, strengthening the data protection mechanisms, ensuring police and criminal justice cooperation and a proper enforcement of the rules on privacy and confidentiality (Heisenberg 2005).

The second problem is security. As experimentally shown by Martinovic et al. (2012), brain-hacking via input manipulation exposes BCI users to the risk of losing surveillance over their personal and financial security. Additionally, the opening of a breach into private and confidential information implied by input-manipulation also exposes users to physical and psychological insecurity. The reason for that stems from the fact that the sort of information potentially extractable from a user's mind does not limit to financial information but may extend to information about the health condition of the users, their profession, location, psychological capacities, sexual preferences, religious beliefs, routine activities etc. For example, Martinovic et al. (2012) have proved the feasibility of extracting information about the user's place of residence and date of birth, two types of information that are directly involved in personal security. It is expected that other types of equally complex information can be extracted in a similar manner (Bonaci et al. 2014). This type of information is potentially of interest not only to criminals involved in harmful activities such as blackmail but also to employers and insurances. For example, health insurance companies may be interested in extracting information about the medical records of the user to accept or reject her enrollment into an insurance plan or to determine her insurance premiums. Similarly, employers could extract information about the user's political views or sexual preferences and commit political or sexual orientation discrimination.

Physical and psychological safety

Brain-hacking via measurement-manipulation, decoding-manipulation, and feedback-manipulation pose a problem for physical and psychological safety. These types of hacking may result in severe physical and psychological (e.g. traumatic experiences) harm to users in a way that is proportionate to the level of benefit of the BCI in assisting the user's physical and psychological performance. For example, patients using BCIs to control wheelchairs may suddenly lose their reacquired spatial mobility and be led back to their original condition of impairment (prior to the BCI). Similarly, robotic limb users and patients using vision BCIs may lose respectively their reacquired motor capacity and visual perception. This sort of attacks require immediate monitoring in the context of security, surveillance and public health as they may not need to involve sophisticated malware development, hence can performed also in absence of specific cybercriminal skills.

In addition, BCI users that are victim of these types of attack may experience psychological distress as a result of their incapacity to perform the actions that they are mentally inducing. This distress would be particularly significant in LIS patients who use BCIs as the only available connection

to the external world.[9] As the primary goal of implementing neurotechnologies in health-care is promoting the benefit of the patient, the development of regulatory mechanisms for protecting physical and psychological safety will be required. Equally strict and rigorous regulatory mechanisms should protect healthy people who use consumer-grade BCI for entertainment, gaming and communication.

Autonomy, agency and personhood

Particularly critical ethical and legal implications are posed by brain-hacking through decoding and feedback-manipulation. The reason for that stems from the fact that these types of brain-hacking, as previously mentioned, would not simply enable malevolent actors to access information but may cause changes in the user's decision-making and/or behavior. This possibility for an external control over the user's future behavior seems to substantially conflict with the moral values of personal autonomy and free agency and may even interfere with the self-determination of personal identity. Personal autonomy is generally understood as the capacity of someone to deliberate or act on the basis of one's own desires and plans and not as the product of manipulative or distorting external forces (Anderson 2013; Buss 2002). Autonomous individuals are those that are able to act freely in accordance with a self-chosen plan. By contrast, potential victims of brain-hacking may see their deliberation and action being partially limited, controlled or interfered by malevolent others. From this perspective, the way brain-hackers influence the users' decisions and behavior seems to substantially undermine their individual autonomy. The threat to autonomy posed by brain-hacking will be exacerbated in the clinical context as it would affect an extraordinarily vulnerable class of individuals such as patients with severe neurological disorders. In medical ethics, autonomy, conceived at minimum as a "self-rule that is free from both controlling interference by others and from limitations" (Varelius 2006), is usually considered a fundamental requirement for the respect of patients and the protection of their dignity (Beauchamp and Childress 2001; Varelius 2006). It is important to stress, however, that although hacked BCI-users with severe neurological conditions would be exposed to the risk of diminished autonomy if compared to non-hacked users with the same condition, they may, nevertheless, achieve greater overall autonomy than equally impaired patients who do not have access to BCI whatsoever. This fact is worth extensive philosophical reflection, since the counterintuitive situation that the same technology can both increase and diminish autonomy requires quite detailed analysis of the benefit-risk ratios in different scenarios.

The challenge to autonomy posed by these types of brain-hacking also raises the issue of coercion, i.e. the exercise of a constraining power on another party (besides the use of force, violence, and threats thereof) with the purpose of forcing him or her to act in a non-voluntary manner (Mill 1869). As such, brain-hacking could raise a novel, more subliminal (since performed below the victim's threshold of consciousness) form of coercion which adds to extortion, blackmail, torture and other currently performed forms of coercion.

Strictly related to the notion of autonomy is the notion of agency, i.e. the capacity of an agent to act, and the capacity to distinguish between events that are self-initiated versus simply occurring (i.e. experiencing the difference between doing something and having something happening to you). The sense of agency serves to identify the range of one's actions (i.e. activities actively performed by agents) from those events that are passively caused by external forces. For example, jumping into the water is considered an action if the jump is performed by the agent without being caused by external forces (e.g. being forced into the water by another person or by the wind). Similarly, controlling a wheelchair via BCI is an action if it is performed intentionally by the agent. In itself, BCI already contains the possibility to result in considerable uncertainty of the BCI user about whether or not the user actually did or did not perform a BCI mediated action, e.g. in case of error (Haselager 2013). When another agent, e.g. a remote hacker, gains control over the application and determines the actions of the user, the agency of the BCI user diminishes and the uncertainty of ascribing the action to the user increases significantly. This is ethically problematic for three major reasons. First, because the detachment of the intention-action causal link prompted by brain-hacking may result in psychological distress and for the user. Second, because it generates uncertainty about the voluntary character of the user's actions. Third and consequently, because in Western jurisprudence the capacity for voluntary control over one's own actions is consider a requisite for legal liability. Therefore, diminished or absent voluntary control over one's own actions would result in diminished or absent legal liability of the user with regard to those actions. This intimate link between agency and legal liability is explicitly expressed by the USA Model Penal Code (MPC), Section 2.01, which states that ''(1) a person is not guilty of an offense unless his liability is based on conduct that includes a voluntary act or the omission to perform an act of which he is physically capable". The MPC also provides a list of examples of non-liable acts which includes: "(a) a reflex or convulsion; (b) a bodily

[9] Here too, there is a difference between hacking by disruption and hijacking, as the psychological stress involved in doing something different from what the user intended may differ from the traumatic experience of losing control over oneself.

movement during unconsciousness or sleep; (c) conduct during hypnosis or resulting from hypnotic suggestion; (d) a bodily movement that otherwise is not a product of the effort or determination of the actor, either conscious or habitual" (Wechsler 1968). The performance of an act as a consequence of brain-hacking via output manipulation seems to fit in at least three of the four above mentioned explicative categories, as the act is not a product or determination of the BCI user but of the hacker. Problems of uncertain legal liability are expected to arise. Collaborative research at the intersection between criminal law, cybersecurity, neurotechnology and ethics will be required in the next future to assess these problems in a manner that facilitates the judicial circuit and protects BCI users.

Conclusions

This paper took a first step in addressing the issue of brain-hacking and raising awareness on the ethical and security implications associated with the malicious use of BCI technology. An overview of the possible vulnerability sources of BCIs and their related sorts of brain-hacking was offered. Additionally, an inventory of the major ethical implications of brain-hacking via BCI was provided. Further interdisciplinary investigation is required to extensively analyze those implications and to develop a normative and regulatory framework that allows maximizing the benefits of BCI technology while minimizing its potential risks.

BCI applications have the potential of significantly improving life quality in patients (especially in patients suffering severe neuromuscular disorders) and enabling enhanced and more personalized user experience in communication, gaming and entertainment for general users. However, the potential benefits of this technology may be tempered if security issues and ethical-legal considerations remain unaddressed. Ideally, this debate should involve the collaboration of ethicists, neuroscientists, engineers, computer scientists, cybersecurity experts, lawyers and other significant stakeholders and inform regulators and policy-makers.

Acknowledgments This project was partly supported by the Erasmus Mundus Scholarship (European Commission).

Compliance with ethical standards

Conflict of interest The authors declare that they have no competing interests.

References

Allison, B. Z., Wolpaw, E. W., & Wolpaw, J. R. (2007). Brain–computer interface systems: Progress and prospects. *Expert Review of Medical Devices, 4*(4), 463–474. doi:10.1586/17434440.4.4.463.

Anderson, J. (2013). Autonomy. In *The International Encyclopedia of Ethics*. Blackwell Publishing Ltd. http://dx.doi.org/10.1002/9781444367072.wbiee716

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics*. New York: Oxford University Press.

Bonaci, T., Calo, R., & Chizeck, H. J. (2014). App stores for the brain: Privacy & security in brain–computer interfaces. In *IEEE international symposium on ethics in science, technology and engineering, 2014*.

Brunoni, A. R., Nitsche, M. A., Bolognini, N., Bikson, M., Wagner, T., Merabet, L., et al. (2012). Clinical research with transcranial direct current stimulation (tDCS): Challenges and future directions. *Brain Stimulation, 5*(3), 175–195. doi:10.1016/j.brs.2011.03.002.

Buss, S. (2002). Personal autonomy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2014 Edition). http://plato.stanford.edu/archives/win2014/entries/personal-autonomy/.

Buxton, M. (1987). *Problems in the economic appraisal of new health technology: The evaluation of heart transplants in the UK* (pp. 103–118). Oxford, England: Oxford Medical Publications.

Chizeck, H. J., & Bonaci, T. (2014). Brain–computer interface anonymizer. Google Patents.

Clausen, J. (2011). Conceptual and ethical issues with brain–hardware interfaces. *Current Opinion in Psychiatry, 24*(6), 495–501.

Conner, M. (2010). Hacking the brain: Brain-to-computer interface hardware moves from the realm of research. *EDN, 55*(22), 30–35.

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: Security and privacy for neural devices. *Neurosurgical Focus, 27*(1), E7.

Dupont, B. (2013). Cybersecurity futures: How can we regulate emergent risks? *Technology Innovation Management Review, 3*(7), 6–11.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper, 1*.

Fazel-Rezai, R., Allison, B. Z., Guger, C., Sellers, E. W., Kleih, S. C., & Kübler, A. (2012). P300 brain computer interface: Current challenges and emerging trends. *Frontiers in Neuroengineering, 5*(14), 14.

Fetz, E. E. (2015). Restoring motor function with bidirectional neural interfaces. *Progress in Brain Research, 218*, 241–252.

Godfrey-Smith, P., & Sterelny, K. (2007). Biological information. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2016 Edition). http://plato.stanford.edu/archives/sum2016/entries/information-biological/.

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights, and regulations*. Hershey, PA: IGI Global. ISBN 978-1-60960-830-9.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., et al. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE symposium on security and privacy, 2008, SP 2008*.

Haselager, P. (2013). Did I do that? Brain–computer interfacing and the sense of agency. *Minds and Machines, 23*(3), 405–418.

Heisenberg, D. (2005). *Negotiating privacy: The European Union, the United States, and personal data protection*. Boulder, CO: Lynne Rienner Publishers.

Kotchetkov, I. S., Hwang, B. Y., Appelboom, G., Kellner, C. P., & Connolly, E. S, Jr. (2010). Brain–computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurgical Focus, 28*(5), E25.

Li, Q., Ding, D., & Conti, M. (2015). Brain–computer interface applications: Security and privacy challenges. In *IEEE conference on communications and network security (CNS), 2015*.

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the feasibility of side-channel attacks with brain–computer interfaces. In *USENIX security symposium*.

Mill, J. S. (1869). *On liberty*. London: Longmans, Green, Reader, and Dyer.

Miranda, R. A., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., et al. (2015). DARPA-funded efforts in the development of novel brain–computer interface technologies. *Journal of Neuroscience Methods, 244*, 52–67.

Powell, C., Munetomo, M., Schlueter, M., & Mizukoshi, M. (2013). Towards thought control of next-generation wearable computing devices. In K. Imamura, S. Usui, T. Shirao, T. Kasamatsu, L. Schwabe & N. Zhong (Eds.), *Brain and Health Informatics* (pp. 427–438). Springer.

Pustovit, S. V., & Williams, E. D. (2010). Philosophical aspects of dual use technologies. *Science and Engineering Ethics, 16*(1), 17–31.

Rosenfeld, J. P. (2011). P300 in detecting concealed information. In Verschuere, B., Ben-Shakhar, G., & Meijer, E. (Eds.), *Memory detection: Theory and application of the concealed information test* (pp. 63–89). Cambridge University Press.

Rosenfeld, J. P., Biroschak, J. R., & Furedy, J. J. (2006). P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms. *International Journal of Psychophysiology, 60*(3), 251–259.

Shannon, C. (1949). *The mathematical theory of environments. The mathematical theory of communication* (pp. 1–93). Urbana: University of Illinois Press.

Strickland, E. (2014). Brain hacking: Self-experimenters are zapping their heads. *IEEE Spectrum, 51*(5), 23–25. doi:10.1109/mspec.2014.6808452.

Tronnier, V. M., & Rasche, D. (2015). Deep brain stimulation. In *Textbook of Neuromodulation* (pp. 61–72). New York: Springer.

Vallabhaneni, A., Wang, T., & He, B. (2005). Brain–computer interface. In *Neural Engineering* (pp. 85–121). New York: Springer.

van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., & Gielen, S. (2009). The brain–computer interface cycle. *Journal of Neural Engineering, 6*(4), 041001.

van Vliet, M., Mühl, C., Reuderink, B., & Poel, M. (2010). Guessing what's on your mind: using the N400 in Brain Computer Interfaces. In Y. Yao, R. Sun, T. Poggio, J. Liu, N. Zhong, J. Huang (Eds.), *Brain Informatics* (pp. 180–191). Berlin Heidelberg: Springer.

Varelius, J. (2006). The value of autonomy in medical ethics. *Medicine, Health Care and Philosophy, 9*(3), 377–388.

Wechsler, H. (1968). Codification of criminal law in the United States: The model penal code. *Columbia Law Review, 68*(8), 1425–1456.

Westby, J. R. (2004). *International guide to privacy*. American Bar Association, Privacy & Computer Crime Committee, and American Bar Association, Section of Science & Technology Law.

Yuan, B. J., Hsieh, C.-H., & Chang, C.-C. (2010). National technology foresight research: A literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy, 6*(1), 5–35.