Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Chapter Five

A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics

Developing a two-dimensional cognitional security framework

In this chapter we develop a two-dimensional conceptual framework for cognitional security. The first dimension includes nine essential information security attributes or goals for neuroprosthetic devices and device-host systems, namely **confidentiality**, **integrity**, **availability**, **possession**, **authenticity**, **utility**, **distinguishability**, **rejectability**, and **autonomy**. Each of these attributes relates to the device-host system as understood at three different levels, which comprise the second dimension of the framework; the levels are those of the device's host understood as **sapient metavolitional agent**, **embodied embedded organism**, and **social and economic actor**. Below we present this framework in detail and consider its implications for information security for advanced neuroprosthetic devices.

Defining security goals for the entire device-host system: nine essential attributes

One of the most fundamental ways of understanding information security is through a framework of essential characteristics that a system must possess in order to be secure. One can understand these characteristics as the security "attributes" that an ideal system would possess. However, in practice such characteristics can never be perfectly achieved, and thus rather than envisioning them as a system's optimal state, they can instead be understood as the security "goals" that one is perpetually striving to attain through the process of information security.

Denning et al. propose a model of "neurosecurity" for neuroprosthetic devices that strives for "the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

safety of a person's neural mechanisms, neural computation, and free will."[1] While that model provides an excellent starting point (especially with regard to contemporary types of neuroprosthetic devices that are already in use), in itself it is not sufficiently specific or robust to drive the development of mature and highly effective information security plans, mechanisms, and practices that will be capable of protecting neuroprosthetic devices and device-host systems from the full range of threat sources, including expertly skilled and intensely motivated adversaries. In particular, a strong and more comprehensive information security framework will be needed to protect the kinds of highly sophisticated (and even posthuman) neuroprosthetic devices and device-host systems that are expected to become a reality within the coming years and decades.

The cognitional security framework that we develop here for a device-host system utilizing advanced neuroprosthetics includes nine security goals or attributes: three are the elements of the classic CIA Triad (confidentiality, integrity, and availability);[2] three are additional characteristics developed by Donn Parker in his security hexad (possession, authenticity, and utility);[3] and three are new characteristics which we have identified as being uniquely relevant for the security of advanced neuroprosthetics (distinguishability, rejectability, and autonomy).[4] Below we briefly define each of these security goals, with particular reference to their relevance for advanced neuroprosthetics.

Confidentiality

In the context of an advanced neuroprosthetic system, we can define confidentiality as "**limiting the disclosure of information to only those sapient agents that are authorized to access it**."

Note that according to this understanding, confidentiality has only been breached if the information is accessed by another "sapient agent" (such as a human being) who is not authorized to do so. For example, imagine that a neural implant is able to detect and record the contents of my thoughts and

---

[1] See Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

[2] Rao & Nayak, *The InfoSec Handbook* (2014), pp. 49-53.

[3] See Parker, "Toward a New Framework for Information Security" (2002), and Parker, "Our Excessively Simplistic Information Security Model and How to Fix It" (2010).

[4] There is ongoing debate about the number and relationship of information security goals and attributes. Other attributes identified by some, such as "completeness" and "non-repudiation/accuracy" (see Dardick's analysis of IQ, CFA, and 5 Pillars in Dardick, "Cyber Forensics Assurance" (2010)) or "accountability" and "assurance" (*NIST SP 800-33* (2001), p. 3) are not explicitly considered here as independent objectives.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

– without my knowledge – is wirelessly transmitting a record of this data to create a "backup copy" of my thoughts on an external computer. While this means that I no longer have sole control or "possession" of the information (as defined below), the creation of such an unauthorized external backup of my thoughts does not in itself represent a loss of confidentiality, as long as the information stored on the external computer is not viewed by some unauthorized person. Confidentiality applies not only to the data stored within a system but also to information about the system itself,[5] insofar as knowledge about a system's design, functioning, and vulnerabilities makes it easier for unauthorized parties to plan an attack on the system.

Our definition of confidentiality in relation to neuroprosthetics builds on existing definitions of confidentiality used in the field of information security. For example, confidentiality has previously been defined as "the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit."[6] Parker defines confidentiality as the "Limited observation and disclosure of knowledge."[7] Alternatively, it can be understood as "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[8] Glenn Dardick proposes a model of Cyber Forensics Assurance (CFA) in which confidentiality is understood as "ensuring that information is accessible only to those authorized to have access."[9]

While ensuring that information is not disclosed to unauthorized parties is typically an important organizational goal, preventing the destruction or corruption of the information is often an even more important objective. Thus *NIST SP 800-33* notes that "For many organizations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g., authenticators), confidentiality is extremely important."[10] As is true for implantable medical devices generally, neuroprosthetic devices constitute a class of systems whose data is often highly sensitive and for which confidentiality is thus a great concern.

---

[5] *NIST SP 800-33* (2001), p. 2.

[6] *NIST SP 800-33* (2001), p. 2.

[7] Parker, "Toward a New Framework for Information Security" (2002), p. 125.

[8] 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37*, Rev. 1 (2010), p. B-2.

[9] Dardick, "Cyber Forensics Assurance" (2010), p. 61. Dardick developed his CFA model by analyzing and synthesizing definitions developed in frameworks such as the CIA Triad as defined in the Federal Information Security Management Act of 2002 (FISMA), the Five Pillars of Information Assurance model developed by the US Department of Defense, the Parkerian Hexad, and the Dimensions of Information Quality developed by Fox and Miller.

[10] *NIST SP 800-33* (2001), p. 2.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Integrity

With regard to an advanced neuroprosthetic system, we can define integrity as "**remaining intact, free from the introduction of substantial inaccuracies, and unchanged by unauthorized manipulation**."

As is true for confidentiality, integrity is needed for both the data stored within a system as well as for the storage system itself.[11] The integrity of information in advanced neuroprosthetic systems is a complex issue, especially in the case of neuroprosthetics that are involved with the mind's processes of forming, storing, and recalling long-term memories. The long-term memories that are stored within our brain's natural memory systems already undergo natural processes of compression and degradation over time;[12] none of our long-term memories presents a perfect replica of the original experience that led to formation of the memory. While our memories may, over time, lose detail and become more impressionistic, they do not lose "integrity" unless the memory has been transformed in such a way that the meaning that it *does* convey is no longer accurate or no longer presents a coherent whole. According to our definition, a memory also does not lose integrity simply as a result of undergoing manipulation, as long as it is a form of *authorized* manipulation that does not introduce substantial inaccuracies. (Thus a neuroprosthetic device that uses some algorithm to compress memories by identifying and preserving essential details while eliminating inessential elements would not necessarily be damaging the integrity of those memories.)

Within more generalized existing frameworks for information security, data integrity has been defined as "the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit," and system integrity has been defined as "the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation."[13] It is alternatively understood as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[14] Parker defines integrity as the "Completeness, wholeness, and readability of information" and the fact that the information remains "unchanged from a previous state."[15] Dardick's synthetic CFA model summarizes the joint concept of "Integrity/Consistency" as the "perceived consistency of actions, values, methods,

---

[11] *NIST SP 800-33* (2001), p. 2.

[12] See Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

[13] *NIST SP 800-33* (2001), p. 2.

[14] 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37* (2010), Rev. 1, p. B-6.

[15] Parker, "Toward a New Framework for Information Security" (2002), p. 125.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

measures and principle – unchanged 'is it true all of the time?' (Verification)."[16] *NIST SP 800-33* suggests that "Integrity is commonly an organization's most important security objective after availability."[17]

Availability

In the context of an advanced neuroprosthetic system, we can define availability as "**the ability to access and experience desired information in a timely and reliable manner**."

This definition of availability differs somewhat from definitions traditionally used in information security. First, it emphasizes that for the user of a neuroprosthetic system, it is not sufficient for information to be stored in a database from which the user can export or save files with particular subsets of information; it is typically important that the user be able to directly *experience* the information as an object of his or her conscious awareness (e.g., sense data that are presented to one's mind to be perceived in the form of percepts or memories that can be recalled and thus "re-experienced" in one's mind at will). Second, this definition emphasizes that it is not sufficient for a user to have access to a vast pool of information, within which the one or two pieces of information that the user would actually like to consciously recall are lost amidst countless streams of information, most of which are at the moment irrelevant to the user's desires. The users of a neuroprosthetic device must be able to quickly and reliably experience in their conscious awareness the particular piece of information that they desire. In the case of some neuroprosthetics, such as an artificial eye that is conveying sense data from the environment, "quickly" experiencing information effectively means that it must be presented in real time.

Ensuring the availability of information involves maintaining both data and the system or systems that contain it and provide it to users. More generalized frameworks for information security have defined availability as the assurance "that systems work promptly and service is not denied to authorized users;" it involves preventing any "unauthorized deletion of data" or other "denial of service or data" that are either inadvertent or intentional in nature.[18] Availability has alternatively been understood as "Ensuring timely and reliable access to and use of information."[19] Parker defines availability simply as the "Usability of information for a purpose."[20] Dardick's synthetic CFA model understands the joint concept of "Availability/Timeliness" as the

---

[16] Dardick, "Cyber Forensics Assurance" (2010), p. 61.

[17] *NIST SP 800-33* (2001), p. 2.

[18] *NIST SP 800-33* (2001), p. 2.

[19] 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37* (2010), Rev. 1, p. B-2.

[20] Parker, "Toward a New Framework for Information Security" (2002), p. 124.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

"the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time)."[21]

NIST SP 800-33 reports that "Availability is frequently an organization's foremost security objective."[22] Placing such a high priority on availability is reasonable, for example, in the case of an advanced neuroprosthetic device that provides its user with real-time sense data or support in cognitive processes such as memory or volition, where the loss of availability of the device and its data at a critical moment could result in injury or death.

The goals of confidentiality, integrity, and availability display a number of mutual interdependencies; for example, if a system's integrity has been lost, its mechanisms for maintaining the confidentiality and availability of its data may no longer be functional or reliable.[23] Some definitions of availability combine two or more different goals by stating that the objective is not only to ensure that data is always available to legitimate users for legitimate purposes but also to ensure that it is always *unavailable* to any person or process that is attempting to use the data (or the larger system) for "unauthorized purposes."[24] In the framework presented here for neuroprosthetic devices, ensuring availability does not involve preventing information from being accessed by unauthorized parties or authorized parties who would attempt to use the information for unauthorized purposes; instead, security goals such maintaining the *possession* and *confidentiality* of information represent those objectives.

Possession

With regard to an advanced neuroprosthetic system, we can define possession as "**holding and controlling the physical substrate or substrates in which information is embodied**."

This definition requires that in order to have possession of information, the user of a neuroprosthetic device must have *sole* possession. If two different parties own physical copies of some information, then it can be said that the information is *available* to both parties but that neither "possesses" it, insofar as neither party, acting individually, has the ability to prevent the creation of additional physical copies of the information or the distribution of such copies to additional parties.

---

[21] Dardick, "Cyber Forensics Assurance" (2010), p. 61.
[22] *NIST SP 800-33* (2001), p. 2.
[23] *NIST SP 800-33* (2001), p. 4.
[24] *NIST SP 800-33* (2001), p. 2.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Within the framework of the classic CIA Triad, possession is not explicitly defined as a freestanding security goal, however it can be understood implicitly as an aspect of confidentiality and, in some cases, a prerequisite for maintaining integrity and availability. Possession is explicitly delineated as an independent security goal in the expanded Parkerian Hexad, where it is defined as "Holding, controlling, and having the ability to use information."[25] Meanwhile, Dardick's synthetic CFA model summarizes the joint concept of "Possession/Control" as relating to the "chain of custody" of information.[26]

Authenticity

In the context of an advanced neuroprosthetic system, we can define authenticity as "**the quality of in fact deriving from the same source or origin that is claimed or supposed to be the information's source or origin**."

For example, the human host and user of a set of two artificial eyes might reasonably assume that the visual sense data presented by the eyes represents an accurate depiction of the physical environment surrounding the eyes' host. If the artificial eyes are presenting the host with the visual experience that he is sitting in his office at work while in fact he has been kidnapped and is sitting in a laboratory in the headquarters of a rival company – with his artificial eyes having been hacked to provide him with a false impression of his surroundings – we could say that the information being provided by the artificial eyes is inauthentic.[27]

On the other hand, if – as an alternative means of taking a "vacation" – a neuroprosthetic device's host had purposefully paid a sensory engineer to provide him with the visual experience of lounging on a tropical beach while in fact he was lying on his couch at home, we might say that this experience was "virtual" or "fabricated," but according to our definition it would not be "inauthentic," because the host knew that the source of his sense data was not an actual physical beach surrounding him.[28] In other words, the host would not be having an experience of lounging on a real beach that is inauthentic but rather an authentic experience of lounging on a virtual beach.

---

[25] Parker, "Toward a New Framework for Information Security" (2002), p. 125.

[26] Dardick, "Cyber Forensics Assurance" (2010), p. 61.

[27] For the possibility that a device designed to receive raw data from the external environment could have that data replaced with other data transmitted from some external information system, see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012). Regarding the possibility of neuroprosthetics being used to provide false data or information to their hosts or users, see also McGee, "Bioelectronics and Implanted Devices" (2008), p. 221.

[28] In a similar way, one might say that a novel which claims to be historically accurate but is full of errors and anachronisms is "inauthentic," while the same work – if explicitly marketed as a work of fantasy and creative fiction – could not be criticized for being "inauthentic."

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Note that according to our definition, in order for some information provided by a neuroprosthetic device to be inauthentic it is not necessarily required that someone has *explicitly claimed* that this particular information is accurate or originates from a source that is not its actual source; it is enough for the device's host or user to *suppose* that the information is originating from some source which is, in fact, not the actual source of the data. If a particular neuroprosthetic device was sold without any claim that it will provide accurate and authentic information, but its human user has utilized the device for some time and has always found it to present an accurate and authentic representation of the physical environment surrounding the user, then the user might understandably come to assume that this will always be the case in the future. If the device were then hacked and began to present the user with a stream of sense data that was inaccurate and did not reflect physical reality, that information could well be described as "inauthentic," from the user's perspective.

Gray areas may especially arise when neuroprosthetics are being purposefully used to immerse their users in fabricated virtual environments. In general, it is more difficult to describe the information presented by a device as "inauthentic" if the user knows that the purpose of the device is to present a fabricated virtual experience, however it is still possible. For example, imagine that all of a multinational company's employees use neuroprosthetic devices that create a shared virtual environment in which employees from around the world can interact. If a hacker were to manipulate the sense data provided to one particular employee so that he or she believed that a coworker had just made a statement within the virtual world which, in fact, the coworker had never made, the contents of that fabricated statement could be understood as inauthentic.

Within the classic CIA Triad, authenticity is not explicitly described as a security goal. It is included in the expanded Parkerian Hexad, where authenticity is defined as the "Validity, conformance, and genuineness of information."[29] Dardick's synthetic CFA model, meanwhile, summarizes the joint concept of "Authenticity/Original" as the "quality of being authentic or of established authority for truth and correctness – 'best evidence' (Validity)."[30]

Utility

With regard to an advanced neuroprosthetic system, we can define utility as "**the state of being well-suited to be employed for a chosen purpose**."

[29] Parker, "Toward a New Framework for Information Security" (2002), p. 125.

[30] Dardick, "Cyber Forensics Assurance" (2010), p. 61.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Information is not inherently useful or non-useful; it possesses utility only with regard to some particular purpose that has been chosen by a sapient agent, such as its human host or user. The same information could be useful to one person in one moment but not useful to a different person or in a different moment.

For example, an artificial eye might generate sense data that is of use to its human host in navigating his or her environment, reading, working at a computer, cooking, or carrying out countless other everyday activities but which is not useful (and may even be distracting and detrimental) if the user is attempting to meditate, sleep, or concentrate on some mental task. Moreover, the device itself ceases to generate information that is even potentially useful when the eyelids in front of it are closed.[31] Other kinds of advanced neuroprosthetics might not generate any information that is immediately useful to their host but may generate vast quantities of biological and diagnostic data that is useful to the team of medical personnel or engineers who are monitoring and controlling a device in order to effectuate some particular outcomes.

The concept of utility is not explicitly incorporated into the classic CIA Triad – though information's potential utility could be understood, for example, as the reason *why* one wishes certain information to be "available." Dardick's synthetic CFA model summarizes the joint concept of "Utility/Relevance" as providing an answer to the question "Is it useful? / is it the right information?"[32] As part of his security hexad, Parker defines utility as the "Usefulness of information for a purpose"[33] – which in the case of an advanced neuroprosthetic could be a purpose defined by the device's human host, by medical personnel or "experiential engineers" who maintain and control the device with the host's permission in order to produce particular effects for the host, or potentially by an individual or organization that has installed the neuroprosthetic without its host's knowledge or permission and which is utilizing the device to advance objectives that it has determined. The latter might be the case, for example, with a neuroprosthetic that is implanted in an infant at the request of its parents, in a comatose individual at the request of his or her guardian, or by a government agency into its military personnel or corporation into employees. In such cases, the questionable legality and

---

[31] Even with the eyelids closed, an artificial eye conveys very basic information about whether the external environment surrounding the host is pitch black, moderately illuminated, or brightly illuminated. In some cases it may be desirable to eliminate the eyelids' ability to close (e.g., in order to blink or while the host is asleep) in order to allow images recorded by the eyes to be stored or transmitted, even if they are not immediately consciously experienced or used by the host himself or herself.

[32] Dardick, "Cyber Forensics Assurance" (2010), p. 61.

[33] Parker, "Toward a New Framework for Information Security" (2002), p. 125.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

ethicality of such operations is not being considered here, only the fact that regardless of by whom or for what purpose a neuroprosthetic has been implanted, the party who has implanted it will see the device's ongoing utility as an objective to be pursued and whose loss would compromise the device's information security.

Distinguishability

In the context of an advanced neuroprosthetic system, we can define distinguishability as "**the ability to differentiate the information to be secured from information possessing a different source or nature**."

In the case of a desktop computer, laptop computer, or mobile device, it is relatively easy to distinguish the system and data whose information security one is seeking to ensure: such devices are discrete units that can be identified and physically separated from their environments. Moreover, it is relatively easy to identify what data is stored on the device, whether it be stored on a magnetic hard drive, flash memory, ROM, or some other physical substrate. By knowing the boundaries of one's system and identifying the information that is to be protected, one can thus develop a clear information security strategy. However, because of their close integration with the human body and human mind's own systems for generating, receiving, storing, transmitting, and processing information, it can be difficult to determine: 1) which are the synthetic systems and neuroprosthetically derived information which the designer, manufacturer, and operator of a neuroprosthetic device may possess the legal and ethical authority to control and manipulate (and for whose security they may bear both legal and ethical responsibility), and 2) which are the natural systems and informational content of the host's biological body and mind – which the operator of a neuroprosthetic device may have a legal and ethical responsibility to keep secure, but without necessarily possessing a legal basis for controlling, manipulating, or even affecting those systems and sources of information.[34] If the information provided by a neuroprosthetic cannot be distinguished from information emanating from other sources, it likely becomes more difficult to ensure the information's security.

Consider a human being who has been implanted with retinal implants that supply the visual sense data constituting 30% of the person's field of vision, while the remaining 70% of the sense data is provided by the person's natural retinal cells. If the person knows which 30% of his field of vision is

[34] In respect to the complex questions that arise regarding who bears moral, legal, and financial responsibility for activities involving implanted ICT devices, see Roosendaal, "Carrying Implants and Carrying Risks; Human ICT Implants and Liability" (2012).

*Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.*

being generated by his neuroprosthetics, his information security situation is qualitatively different from that of a person who knows that 30% of his field of vision is being provided by an artificial device but does not know *which portion* of his field of vision is "synthetic" and which is "natural." Similarly, the user of a mnemocybernetic implant who is able to easily distinguish (e.g., through some ineffable inner sensation or awareness) the mnemonic content provided by the implant from the mnemonic content stored in his or her brain's natural memory systems faces a different information security situation than someone who knows that he or she possesses a mnemonic implant but has no way of distinguishing memories stored in the implant from memories stored in the natural mechanisms of his or her brain – and different still is the situation of someone who does not even realize that he or she possesses a mnemonic implant and who is not even aware that he or she should be *attempting* to distinguish between those memories that are natural and those that are neuroprosthetically generated.

Rejectability

With regard to an advanced neuroprosthetic system, we can define rejectability as "**the ability to exclude particular information from one's conscious awareness on the basis of its source, nature, or other characteristics**."

It is important to ensure that information is available whenever its user wishes to access it. However, in the case of a neuroprosthetic device it is at least as important to ensure that the information is not involuntarily forced into the mind of its host or user when he or she *does not* wish to access it.

The ability of advanced neuroprosthetics to forcibly inject experiences – whether sense data, memories, emotions, or other mental phenomena – into the conscious awareness of their host or user makes it essential that such devices have safeguards to guarantee that their users are not subject to sensory overload, brainwashing, or other kinds of psychological or emotional assault. This becomes particularly important if, for example, a neuroprosthetic device has been implanted in a child, an individual suffering motor impairments, or other persons who many not be able to actively adjust or disable the device or express their lack of consent to the experience. Cognitional security involves not only being able to bring desired information into one's mind for use but also to keep it out of one's mind, when desired.

Autonomy

In the context of an advanced neuroprosthetic system, we can define autonomy as "**the state of a subject that consciously experiences its own use of information and which possesses and exercises agency in generating information**."

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

This is clearly not an attribute that applies to information stored in a traditional system, such as the hard drive of a desktop computer. In that case neither the information itself nor the computer system containing the information possesses a subjective experience of the information, and if the computer can be said to exercise "agency" in generating information, it is only in a limited sense (at least, in comparison to human beings), insofar as a conventional computer does not possess its own desires, beliefs, volitions, or conscience.[35]

In the case of a human being implanted with an advanced neuroprosthetic device, the information contained within the device does not, in itself, possess autonomy. However, unless he or she is in a comatose state and thus deprived of the ability to consciously experience information or utilize agency in generating it, the potential human host of a neuroprosthetic device *does* possess informational autonomy in the sense defined above, and the integration of the neuroprosthetic device into the host's neural circuitry to create a new device-host system should not be allowed to impair or destroy the host's informational autonomy. In this sense, we can say that preserving the informational autonomy of the device-host system is an important goal of information security. Autonomy is thus the epitome of a new kind of security goal and attribute that has not been relevant for the information security of traditional computerized data-storage systems but which becomes relevant – and, indeed, assumes paramount importance – in the case of information stored within an advanced neuroprosthetic and the system that it forms with its human host.

When working to ensure the security of information contained within a hard drive, the hard drive does not possess its own rights or human welfare about which we must be concerned. Similarly, a computer running the most sophisticated sorts of artificially intelligent software available today may demonstrate a limited form of agency, but such a platform is not a moral agent that is capable of possessing its own conscience (or "metavolition") or conscious awareness, nor is it (like infants or at least some animals) the sort

[35] For the extent to which it is possible for technological devices – whether a conventional desktop computer or a far more sophisticated construct such as a social robot or artificial general intelligence (AGI) – can possess and demonstrate agency and autonomy and the forms that these traits can take, see, e.g., Coeckelbergh, "From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots" (2011); Calverley, "Imagining a non-biological machine as a legal person" (2008); Hellström, "On the Moral Responsibility of Military Robots" (2013); Kuflik, "Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?" (1999); Stahl, "Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency" (2006); and Friedenberg, *Artificial Psychology: The Quest for What It Means to Be Human* (2011).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

of "moral patient" about whose welfare human beings must be concerned even though it is not in itself a moral agent. Thus in certain circumstances it may be appropriate to destroy a hard drive or computer as part of an overall strategy for keeping secure the information contained within it. However, in the case of a neuroprosthetic device, maintaining the biological and psychological welfare of the being into whose organism and mind the device is integrated is typically the greatest priority, and any efforts at securing the neuroprosthetic device and information contained within it must not be allowed to impair the wellbeing of the device's human host.

Note that there is not simply a danger that a device's built-in information security mechanisms might harm its host; it is also possible that the device's mere presence might damage the mind of its host and the information contained within that mind. Especially in the case of neuroprosthetics that affect their host's processes of memory,[36] volition, metavolition,[37] emotion,[38] and conscious awareness,[39] there is a possibility that the device might negatively impact the host's possession and exercise of the autonomy, moral agency, consciousness, and conscience that are among the defining traits of a human being.

It is possible to conceive of an invasive neuroprosthetic device which, for example, replaces sections of the host's brain in a way that destroys the host's conscious awareness while replacing it with an AI-driven artificial agency contained in the device.[40] Such concerns regarding authenticity and personal identity have already been expressed regarding neural implants used for deep brain stimulation to treat conditions such as Parkinson's disease.[41] We can

---

[36] For the possibility of developing mnemoprosthetics, see Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

[37] See, for example, Negoescu, "Conscience and Consciousness in Biomedical Engineering Science and Practice" (2009), and Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

[38] For the possibility of developing emotional neuroprosthetics, see Soussou & Berger, "Cognitive and Emotional Neuroprostheses" (2008); Hatfield et al., "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior" (2009); Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011); McGee, "Bioelectronics and Implanted Devices" (2008), p. 217; and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[39] For the possibility of neuroprosthetic devices relating to sleep, see Claussen & Hofmann, "Sleep, Neuroengineering and Dynamics" (2012), and Kourany, "Human enhancement: Making the debate more Productive" (2013), pp. 992-93.

[40] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015), and Gladden, "'Upgrading' the Human Entity..." (2015).

[41] For the effects of existing kinds of neuroprosthetic devices on the agency (and perceptions of agency) of their human hosts, see Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011), and Berg, "Pieces of Me:

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

summarize these concerns and this security goal by stating that a neuroprosthetic device should support rather than impair the autonomy of its human user.

Prioritizing the information security goals

Parker notes that – however many security attributes one might define – they should be placed in some logical order (such as their order of importance) that adds an additional level of meaning to the list of attributes.[42] If we were to arrange our nine security goals in order of importance as seen from the perspective of a generic neuroprosthetic device-host system (and in particular, a host's conscious awareness), a ranking that appears reasonable would be:

- **Autonomy** of the device-host system, insofar as a neuroprosthetic device and system that impairs its host's autonomy, agency, conscience, and conscious awareness may actually destroy the most fundamental ability of its hostmind to experience and use information, thereby rendering all of the other security attributes irrelevant.
- **Rejectability**, as the ability of a hostmind to *block out* a stream of information that is causing ongoing pain, sensory overload, or physical or psychological trauma is arguably more important than the mind's ability to *access* information that is beneficial and useful.
- **Integrity**, which, if lost, would likely diminish or destroy information's utility and authenticity and render possession of the information of little value.
- **Utility**, as there is little need to ensure, e.g., the availability or possession of information if it is ultimately of no use to the neuroprosthetic device's user.
- **Availability**, which may be crucial for information provided by some neuroprosthetics (e.g., sense data provided by an artificial eye should be in real time, in order to synchronize with data provided by other sensory organs and allow real-time motor control) but less important for information provided by others (e.g., a delay in pulling up certain kinds of long-term memories stored in a memory implant may be permissible).

On Identity and Information and Communications Technology Implants" (2012).

[42] Parker, "Our Excessively Simplistic Information Security Model and How to Fix It" (2010), p. 17.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

- **Confidentiality**, insofar as a neuroprosthetic device may potentially allow outside agents to access the contents of its user's volitions, memories, emotions, and other intimate mental processes whose contents the user would very much like to keep private.
- **Authenticity**, insofar as information that is "false" or "inauthentic" (e.g., fabricated sense data that intentionally misleads the device's user into believing that he is walking through a forest while in fact he is lying on a bed in a hospital) may still be of great value to the device's host and operator as long as it is useful and available.
- **Possession**, as the long-term holding and control of some information provided by neuroprosthetics (such as long-term memories) may be important, but the ability to store long-term and to control of other kinds of information (such as a complete permanent record of all the visual information that one has experienced through one's retinal implants) that are generally experienced by the mind only instantaneously is something that human beings do not currently enjoy and may not expect.
- **Distinguishability**, insofar as it may not be important to distinguish neuroprosthetically supplied from naturally supplied information, as long as the neuroprosthetically supplied information possesses all of the other security attributes. However, distinguishability becomes an important tool that is useful for pursuing information security in cases where other attributes are lacking and specific vulnerabilities, threats, or risks need to be addressed.

Note that if one accepts this ordering, two of the three new security goals for advanced neuroprosthetics that have been introduced in this chapter turn out to be more important than any of the goals traditionally defined in the CIA Triad and Parkerian Hexad. This highlights the danger of assuming that security goals that were developed with previous standalone computer systems (e.g., desktop or laptop computers) in mind will provide an adequate basis for ensuring information security for new kinds of neuroprosthetic devices that are intimately interconnected with the biological and mental processes of a human user. This underscores the need to develop new and more robust "cognitional security frameworks" for such brain-machine interfaces.

Although the ranking of security attributes just proposed appears reasonable as a generic approach, many alternative rankings are possible. While Parker seems to suggest that there may be a single most logical way of ordering

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

security attributes,[43] other experts note that different organizations will prioritize security attributes in different ways,[44] based on each organization's unique mission and the role that information and information technology play within it. In the case of an advanced neuroprosthetic system, any prioritized ordering of security attributes includes many implicit value judgments about the relative importance of various objectives, and different individual hosts or users of neuroprosthetic implants might rank the attributes in quite different ways.

For example, for some device hosts who are powerful political figures or business leaders, ensuring the confidentiality of information contained within their minds might be the ultimate priority, insofar as that information may include classified national security plans that must not be allowed to fall into the hands of hostile states or trade secrets that could be exploited by competing firms; moreover, the person's mind may contain information (e.g., long-term memories dating back to childhood) which, if acquired by unauthorized parties, could provide a basis for blackmail, extortion, or other illicit manipulation. On the other hand, other users might be willing to accept a loss of confidentiality, if in return their neuroprosthetics would grant them new sensorimotor or cognitive capacities, allow them to interact socially in new ways, or provide them with other advantages that outweigh the loss of confidentiality. Indeed, there is even reason to believe that over time, some human beings may come to embrace the use of neuroprosthetics that allow members of a community to mutually experience one another's thoughts – thereby purposefully reducing the confidentiality of information contained within their minds in order to forge new kinds of political dialogue and social relations; in such cases, a loss of confidentiality could be experienced as something "liberating" that advances openness and honesty rather than something frightening and oppressive.[45]

Similarly, some users may give paramount value to the authenticity of the information being conveyed by their neuroprosthetic device. Such users might prefer to have an artificial eye which, for example, provides them with a stream of low-resolution visual sense data that is not particularly useful but which they know is "authentic" (i.e., it accurately reflects the objective physical reality of the environment surrounding them) rather than to possess an artificial eye that provides flawless high-resolution video but which can easily

---

[43] Parker, "Our Excessively Simplistic Information Security Model and How to Fix It" (2010), p. 17.

[44] *NIST SP 800-33* (2001), p. 2.

[45] See Gladden, "'Upgrading' the Human Entity..." (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

be hacked by unauthorized parties – so that the device's user never knows whether the world that they are seeing actually exists or whether it is a false or virtual environment that they are experiencing as a result of fabricated sense data that is being fed to their neuroprosthetic device by a malicious hacker.

When prioritizing the information security goals for a particular advanced neuroprosthetic system, the system's designer should thus take into account factors such as:

- The **market segment(s) of potential users** at whom the device is being targeted.
- The unique information security **needs and concerns** displayed by those groups.
- The ways in which the information security characteristics of the neuroprosthetic device itself, physical maintenance services, software updates, and other products and services offered by the manufacturer will **integrate with the existing information security systems**, services, and priorities maintained by institutions (such as an employer, school, health care provider, or government agency) that already bear responsibility for ensuring those users' information security.

Moreover, in order for the potential user of a neuroprosthetic device to choose the device that is best for him or her and to provide informed consent for its implantation, the relative prioritization of information security goals that have been incorporated into the device's design and functioning should be disclosed to the potential user in the relevant marketing materials and pre-implantation counseling.

Understanding the security goals at three levels

The human host of an advanced neuroprosthetic device intertwines his or her personal informational security with that of the system on different levels, each of which has distinct information security challenges and characteristics

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

that must be taken into consideration.[46] We must consider the neuroprosthetically enabled human being on at least three different levels:[47]

1) The human being as a **sapient metavolitional agent**, a unitary mind that possesses its own conscious awareness, memory, volition, and conscience (or "metavolitionality"[48]).
2) The human being as an **embodied embedded organism** that inhabits and can sense and manipulate a particular environment through the use of its body.
3) The human being as a **social and economic actor** who interacts with others to form social relationships and to produce, exchange, and consume goods and services.[49]

---

[46] Note that while considering the human host of a neuroprosthetic device separately as a sapient mind, embodied biological organism, and social and economic actor is useful for ensuring that one does not overlook any of the information security issues that become especially apparent when considering the human host in one of those capacities, in reality these three roles are always fused and deeply interrelated, if not wholly inextricable from one another. In future posthuman contexts in which very sophisticated neuroprosthetic devices have been deployed, it may sometimes be clear, for example, that a particular human being has become "infected" by a particular *idée fixe* that occupies all of his or her thoughts or wrapped up in a relationship (such as one of love, loyalty, or hatred) that consumes all of the person's energy and attention – but it may be unclear whether the source of the phenomenon – the "vector" that introduced it into the person's life and being – was a biological vector (such as a biological virus or biochemical agent that has affected the person neurologically or physiologically), an electronic vector (such as glitches that occurred in the gathering of sense data or storage of memories by an implant or a computer worm or virus that has infected the synthetic components of the device-host system), or a social vector (such as acts of inspiration, persuasion, seduction, blackmail, or myth-building performed by other intelligent agents and directed at the person). For a use of actor-network theory (ANT) to explore the ways in which, for example, a single "idea" might manifest itself through diverse biological, mental, technological, and social phenomena or activity and the complexities involved with untangling biological and technological symbioses and power relations within such a posthuman context, see Kowalewska, "Symbionts and Parasites – Digital Ecosystems" (2015).

[47] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015). The reminder of this chapter draws heavily on that work.

[48] See Calverley, "Imagining a non-biological machine as a legal person" (2008), for an explanation of the relationship of second-order volitions to conscience and Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015), for use of the word "metavolitional" in this context regarding to neuroprosthetic devices.

[49] The financial and economic aspect of a neuroprosthetic device's impact is important, insofar as financial considerations influence the kind and degree of security measures that can be implemented by individual or institutional users of neuroprosthetic devices, and efforts to compromise information security and illicitly acquire information often have a financial component (e.g., as part of a planned scheme for blackmail, corporate espionage, or sale of the information).

*Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.*

At each of these three levels, a neuroprosthetic device integrates with its host's own natural capacities to create a device-host system whose unique characteristics may create powerful new tools that can assist with ensuring the system's information security, dramatic new vulnerabilities that undermine the system's information security, or both. Below we consider some new capacities and limitations that a neuroprosthetic device can provide its human host at each of the three levels and describe the impact that these new characteristics can have on pursuit of the nine security goals.

Functional vs. information security impacts

Note that there is no direct correlation between a neuroprosthetic device having an *overall functional impact* on its host that is considered positive or negative and its having a more specific *information security impact* that is considered positive or negative. Some of the new neuroprosthetically facilitated characteristics which might be considered *beneficial* from the host or user's perspective (due to the new functional capacities that they provide) may be considered harmful and disadvantageous from the perspective of the InfoSec professionals who are charged with ensuring the host's information security, insofar as the characteristics create egregious new vulnerabilities. Conversely, some feature of a neuroprosthetic device that is generally considered undesirable from the perspective of its host (because it limits or constraints the host in some way) might be considered advantageous from an information security perspective, insofar as it provides a new layer of defense that protects information contained within the host's biological systems or mental processes from access by unauthorized parties.

Impacts on a host vs. impacts on a user

Note also that the impacts that a particular neuroprosthetic device has on the information security of its human *host* may differ significantly (and even be diametrically opposed to) the impacts that it has on the information security of its operator or *user*, if the host and user are different persons. In cases where the host and user are different individuals, this cognitional security framework should be applied separately to the device's host and its user and due attention should be paid to the impacts result for each person.

The human host as sapient metavolitional agent

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Functional capacities created by a neuroprosthetic device

Below we describe some of the new functional capacities that a neuroprosthetic device can provide its host or user in his or her role as a sapient metavolitional agent and the potential impact that these capacities might have on the information security of the host-device system.[50]

Enhanced memory, skills, and knowledge stored within the mind (engrams)

Building on current experimental technologies that are being tested in mice, future neuroprosthetics may offer human users the ability to create, alter, or weaken memories that are stored in their brains' natural memory systems in the form of engrams.[51] This could potentially be used not only to affect a user's declarative knowledge but also to enhance motor skills or reduce learned fears.

Tremendous technological challenges would need to be overcome in order to someday develop a neuroprosthetic device that allows for the precise "editing" of extant human memories or creation of complex new memories within the brain's naturally existing memory systems. Indeed, the exact structures and processes used by the brain to encode, store, and retrieve long-term memories are still shrouded in mystery, and researchers have proposed divergent theories to account for the way in which the brain stores engrams.[52] If, for example, a model such as the Holonomic Brain Theory is correct, then any efforts to make precise adjustments to existing memories by manipulating neurons in a particular portion of the brain may prove futile, as each memory may be stored holographically across the brain's entire neural network.[53] Although researchers have succeeded in understanding many of the large-scale synaptic structures and basic electrochemical functioning of neural synapses – and are making rapid progress at developing artificial neurons that can replicate key elements of this observed synaptic functioning – there is still considerable debate about the extent to which these simple, large-scale

---

[50] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[51] See Han et al., "Selective Erasure of a Fear Memory" (2009); Ramirez et al., "Creating a False Memory in the Hippocampus" (2013); McGee, "Bioelectronics and Implanted Devices" (2008); and Warwick, "The cyborg revolution" (2014), p. 267.

[52] See, for example, Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

[53] See Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

synaptic structures and actions within the brain are responsible for the creation, storage, and recall of long-term memories.[54] Elements of the Holonomic Brain Theory, for example, suggest that much more sophisticated and difficult to observe interactions between neurons (such as those within the "synaptodendritic web"[55]) – may play essential roles in the memory process that we have barely begun to comprehend. The development of a neuroprosthetic device that can successfully integrate with the brain's neural circuitry in order to support, expand, control, or replace the brain's natural mechanisms for creating, storing, and recalling complex engrams is not expected to occur soon, and – depending on which theories of the brain's memory processes prove correct – it may not even be theoretically possible at all.

However, if one assumes that such a technology could be developed, it is clear that it would have major implications for the security of information held within the long-term memory of its host and user. If a device allowed external agents to access and copy the mind's engrams, this would imperil that information's **confidentiality** as well as the host's **possession** of it. The ability to edit or delete existing engrams would threaten the information's **integrity**, **utility**, **availability**, and **authenticity** for the host. If the device were able to forcibly recall particular memories to the host or user's conscious awareness against his or her will, it would undermine the **rejectability** of that information. If the device gave an external agent the wholesale ability to delete, replace, or manipulate the host's memories, this could potentially reduce the host's **autonomy** by eliminating his or her own ability to exercise agency in generating mnemonic contents. If the device were integrated seamlessly into the brain's natural mnemonic systems, from the host and user's perspective the (potentially inauthentic) memories generated by the neuroprosthetic device might lack **distinguishability** from natural memories that were generated by some actual experience in the host's past.

Enhanced creativity

A neuroprosthetic may be able to enhance a mind's powers of imagination and creativity[56] by facilitating processes that contribute to creativity, such as stimulating mental associations between unrelated items. Anecdotal increases in creativity have been reported to result after the use of neuroprosthetics for deep brain stimulation.[57]

---

[54] For example, see Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

[55] See Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

[56] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), pp. 23-24.

[57] See Cosgrove, "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation" (2004), and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement"

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

If such a device were able to force new thoughts into its host's mind against his or her will, that information would lack **rejectability**, and the device might undermine **autonomy** by interfering with or overriding the host's ability to generate his or her own creative thoughts. Moreover, by forcing unwanted and distracting memories into the host's conscious awareness, this could interfere with the host's efforts to access *other* information contained within his or her memory, thereby reducing the **availability**, **utility**, and potentially **integrity** of the latter information. If the host could never be sure whether new ideas had been generated by his or her own imagination or by the device, those ideas would lack **distinguishability**. The ability of outside agents to access ideas generated by the device would undermine that information's **confidentiality** and the host's **possession** of it.

Enhanced emotion

A neuroprosthetic device might provide its host with more desirable emotional dynamics and behavior.[58] Effects on emotion have already been seen, for example, with devices used for deep brain stimulation.[59]

If such a device allowed external agents to detect the host's internal emotional states, the device would be undermining the user's **possession** and the **confidentiality** of that information. If the device could force emotional content into the host's conscious awareness, that information would lack **rejectability** and could undermine the host's **autonomy**. Insofar as such involuntary emotional dynamics distort or render impossible the host's ability to efficiently access and use other information, the **availability**, **utility**, and perhaps **integrity** of such information would suffer.

On the other hand, in the case of a host whose previous severe emotional disturbances had made it difficult or impossible for the person to calmly and efficiently access utilize information contained within his or her memory or provided by the external environment, the use of such a device could potentially *enhance* the **availability** and **utility** of such information. If a person is prone to fits of uncontrollable anger, jealousy, or pride during which he or she lashes out and reveals his or her deepest and harshest criticisms of others or other personal secrets, the use of a neuroprosthetic device to limit such frustrations and outbursts could aid the person in maintaining the **confidentiality** and **possession** of information which, in moments of greater rationality,

---

(2012).

[58] McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

[59] See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

the person would admit that he or she has no desire to reveal. By giving the user greater control over his or her emotions, such a device could enhance the person's own agency (and thus informational **autonomy**) and increase the **rejectability** of unwanted thoughts and feelings that the user was previously unable to block out of his or her mind.

Enhanced conscious awareness

Research is being undertaken to develop neuroprosthetics that would allow the human mind to, for example, extend its periods of attentiveness and limit the need for periodic reductions in consciousness (i.e., sleep).[60]

By enhancing the mind's attentiveness and ability to spend extended periods of time focused on accessing and processing information, such a device could indirectly enhance the **availability** and **utility** of information for its host. Enhancing and extending the host's conscious awareness could also temporally expand (if not otherwise qualitatively change) the host's ability to exercise agency and **autonomy** in the accessing and use of information. On the other hand, if the device is capable of forcibly compelling the host to focus his or her conscious awareness on a particular piece of information, that would limit the **rejectability** of that information and weaken the host's **autonomy**. Moreover, if the device could be misused to *reduce* the host's conscious awareness, this would impair his or her ability to subjectively experience information and thus reduce the host's **autonomy**.

Enhanced conscience

If a "volition" is understood as a belief about the outcome of some action and a desire for that outcome,[61] then one's conscience can be understood as one's set of second-order volitions or "metavolitions," desires about the kinds of volitions that one wishes to possess.[62] Insofar as a neuroprosthetic device enhances processes of memory and emotion[63] that allow for the development of one's conscience, the device may enhance one's ability to develop, discern, and follow one's conscience.[64]

A neuroprosthetic device that is capable of altering a host's most fundamental desires and assessment of what is "right" and "wrong" would have major implications for information security – most noticeably in either strength-

---

[60] Kourany, "Human enhancement: Making the debate more Productive" (2013), pp. 992-93.

[61] Calverley, "Imagining a non-biological machine as a legal person" (2008), pp. 528-30.

[62] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

[63] Calverley, "Imagining a non-biological machine as a legal person" (2008), pp. 532-34.

[64] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

ening or undermining the host's informational **autonomy** and potentially impairing the **integrity** and **availability** of the information that would be conveyed by the host's unaugmented conscience in the absence of such a device. By affecting the host's metavolitions, such a device would over time alter the **rejectability** and availability of information contained in the host's first-order volitions. If such a device provides the host with metavolitions that are determined by (and thus known to) some external agency, the host's previous metavolitions (over which he or she presumably exercised **possession** and sole control) would be replaced by new metavolitions lacking **confidentiality** and sole **possession** by the user.

Functional impairments created by a neuroprosthetic device

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host at the level of his or her internal mental processes and the impact that these impairments might have on the information security of the host-device system.[65]

Loss of agency

A neuroprosthetic may damage the brain or disrupt its activity in a way that reduces or eliminates the ability of its human user to possess and exercise agency.[66] Moreover, the knowledge that this can occur may lead users to doubt whether their volitions are really "their own," an effect that has been seen with neuroprosthetics used for deep brain stimulation.[67]

A neuroprosthetic device that produces a general loss of agency would clearly have a negative impact on its host's informational **autonomy** by reducing the host's ability to possess and exercise agency in generating information. It could also indirectly reduce the **rejectability** of unwanted information and the **availability** of desired information.

Loss of conscious awareness

A neuroprosthetic may diminish the quality or extent of its host's conscious awareness, e.g., by inducing daydreaming or increasing the required amount of sleep. A neuroprosthetic could potentially even destroy its user's

---

[65] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[66] McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

[67] See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

capacity for conscious awareness (e.g., by inducing a coma) but without causing the death of his or her biological organism.[68]

A neuroprosthetic device that produces a loss of conscious awareness on the part of its host would have a negative impact on its host's informational **autonomy** similar to that produced by a loss of agency; if the host's ability to subjectively experience information is completely destroyed, then other attributes such as the **integrity**, **utility**, and **availability** of information for that host would become largely irrelevant, as there would no longer *be* a "host" to whom the information could be presented.

Dependency of internal cognitive processes on external systems

Although the portion of a neuroprosthetic device that directly interfaces with its host's neural circuitry may be implanted in the host's body, it is possible that internal processing, memory, and power constraints may force the device to regularly offload some information to an external system for processing (e.g., through a wireless data link) or to receive instructions from the external system; in this way, the "internal" cognitive processes of the device's host may no longer be taking place solely within the relatively easily protected space of the host's brain and body but within an array of physically disjoint systems that communicate through channels that may be subject to accidental disruption or intentional manipulation.

The restructuring of the host's cognitive processes in such a way increases the possibility of a loss of **autonomy** and reduction in the **integrity**, **availability**, **confidentiality**, **authenticity**, and **possession** of information contained in those cognitive processes. On the other hand, use of external systems to support or create a "backup copy" of the host's internal cognitive processes could potentially also aid in the diagnosis and treatment of cognitive disorders, increased efficiency and power in the mind's cognitive processing, and the restoration of information that otherwise would have been lost to or by the brain's internal cognitive processes – all of which might contribute to an increase in **autonomy** and the **integrity**, **availability**, and **utility** of information.

Inability to distinguish a real from a virtual ongoing experience

If a neuroprosthetic device alters or replaces its host's sensory perceptions, it may make it impossible for the user to know which (if any) of the sense data that he or she is experiencing corresponds to some actual element of an external physical environment and which is "virtual" or simply "false."[69]

---

[68] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

[69] For the possibility that a device designed to receive raw data from an external environment could have that data replaced with other data transmitted from some external information system, see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Ad-

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Such a neuroprosthetic device would certainly produce a loss of **distinguishability** in the sensory information experienced by its host and would open the door to external manipulation that could reduce the **availability** of accurate information that the host was blocked from seeing and the **authenticity** and **utility** of the information that was instead received by the host.

Inability to distinguish true from false memories

If a neuroprosthetic device is able to create, alter, or destroy engrams within its host's brain, it may be impossible for a host to know which of his or her apparent memories are "true" and which are "false" (i.e., distorted or purposefully fabricated).[70]

This kind of neuroprosthetic device would produce a loss of **distinguishability** in the mnemonic information experienced by the host and could facilitate external manipulation that could reduce the **availability** of accurate mnemonic information that the host was blocked from recalling and the **authenticity** and **utility** of the information that was instead recalled by the host. It could also impair the host's **autonomy**, insofar as he or she may be exercising agency and making decisions based on memories that are not actually his or her own.

Other psychological side-effects

A host's brain may undergo potentially harmful and unpredictable structural and behavioral changes as it adapts to the presence, capacities, and activities of an advanced neuroprosthetic device.[71] These effects may even include new kinds of neuroses, psychoses, and other disorders unique to hosts or users of advanced neuroprosthetics.

Depending on their nature and severity, such changes could negatively impact hosts' **autonomy** and the **rejectability**, **integrity**, **utility**, **availability**, **authenticity**, and **distinguishability** of information experienced by the hosts or users, as well as potentially leading hosts to involuntarily disclose information in a way that damages its **confidentiality** and the hosts' **possession** of it.

---

vantage of Bionic Ears and Eyes" (2012). Regarding the possibility of neuroprosthetic devices being used to provide false data or information to their hosts or users, see also McGee, "Bioelectronics and Implanted Devices" (2008), p. 221. See also Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

[70] See Ramirez et al., "Creating a False Memory in the Hippocampus" 2013.

[71] See McGee, "Bioelectronics and Implanted Devices" (2008), pp. 215-16, and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 125, 130.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

On the other hand, it is also possible that the structural and behavioral changes occurring in a host's brain as the result of using an advanced neuroprosthetic might have salutary effects that increase the host's **autonomy**, enhance the **integrity**, **availability**, and **utility** of information, and strengthen the host's ability to maintain the **confidentiality** and **possession** of that information. The designers of neuroprosthetic devices will need to conduct careful monitoring and testing to identify the short- and long-term effects of the devices' use and discover potentially unexpected side-effects that may have an impact on information security.

The host as embodied embedded organism

Functional capacities created by a neuroprosthetic device

Below we describe some of the new functional capacities that a neuroprosthetic device can provide its human host or user in his or her role as an embodied embedded organism and the potential impact that these capacities might have on the information security of the host-device system.[72]

Sensory enhancement

A neuroprosthetic device may allow its host or user to sense his or her physical or virtual environment in new ways, either by acquiring new kinds of raw sense data or new modes or abilities for processing, manipulating, and interpreting sense data.[73]

The **availability**, **integrity**, **utility**, and **authenticity** of information provided by such devices depends not only on their quality and technical specifications but also on securing the devices from external manipulation. If the sense data that is being gathered by the devices and transmitted to the user's mind can be intercepted by external agents, the **confidentiality** and **possession** of that information is undermined. Such devices also raise questions of **rejectability** if the user cannot block out the information that they provide. The extent to which information provided by the neuroprosthetic device displays **distinguishability** from the user's other natural sensory input may depend not only on the device's technical capacities and limitations but also on explicit design decisions made by the device's producer about the ways in which information should be presented. Insofar as such devices might expand the capacities of their users to consciously experience sense data and make decisions on the

---

[72] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[73] See Warwick, "The cyborg revolution" (2014), p. 267; McGee, "Bioelectronics and Implanted Devices" (2008), p. 214; and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 120, 126.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

basis of it, such devices could potentially enhance their users' agency and **autonomy**.

Motor enhancement

A neuroprosthetic device may give its host or user new ways of manipulating physical or virtual environments through his or her body.[74] For example, it might grant enhanced control over one's existing biological body, expand one's body to incorporate new devices (such as an exoskeleton or vehicle) through body schema engineering,[75] or allow the user to control external networked physical systems such as drones or 3D printers or virtual systems or phenomena within an immersive cyberworld.

Insofar as such mechanisms for motor enhancement provide proprioceptive or other sensory feedback, they would be subject to the issues noted above for neuroprosthetics that provide sensory enhancement. Neuroprosthetics that provide strengthened control over a host's body could enhance the **confidentiality** and **possession** of information by their hosts by preventing the inadvertent disclosure of information through motor actions such as speech or facial expressions. On the other hand, by extending or altering the host or user's body, such a device might simply create new motor avenues through which such information can be inadvertently disclosed.

Enhanced memory, skills, and knowledge accessible through sensory organs (exograms)

A neuroprosthetic device may give its user access to external data-storage sites whose contents can be "played back" to the user's conscious awareness through his or her sensory organs or to real-time streams of sense data that augment or replace one's natural sense data.[76] The ability to record and play back one's own sense data could provide perfect audiovisual memory of one's experiences.[77]

Neuroprosthetics that store memories, skills, and other information as exograms[78] that are external to the brain's own natural mnemonic systems face

---

[74] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 213, and Warwick, "The cyborg revolution" (2014), p. 266.

[75] See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics..." (2015).

[76] See Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 115, 120, 126.

[77] See Merkel et al., "Central Neural Prostheses" (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

[78] E.g., devices of the sort described by Werkhoven, "Experience Machines: Capturing and Retrieving Personal Content" (2005), but in implantable rather than external wearable form.

*Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.*

different information security issues from those that store information in the form of engrams within the brain's natural mnemonic mechanisms. Information stored within engrams can be recalled by the user's mind without first needing to pass through sensory organs; the information appears to come "from within" the user's own mind, rather than being presented to the user's conscious awareness through the use of sensory organs as if the information were originating from some environment outside of the user's mind. The fact that the use of engrams bypasses the brain's sensory systems creates different information security capacities and concerns than the use of exograms that must be presented through sensory organs or sense modalities.

Because information stored as exograms can potentially take the form of conventional text, video, audio, or image files (rather than being stored as patterns of interconnection, activation functions, and learning processes within a neural network), it may be easier for unauthorized parties to access, manipulate, delete, or replace that information. On the other hand, the ability to store information in conventional file formats may allow the use of encryption and other security or access controls that are not possible for information stored as engrams within the brain's own neural networks – since information stored within the brain's own mnemonic systems must utilize whatever form and structure the brain is designed to handle rather than whatever more "secure" structures a security-conscious neuroprosthetic engineer might wish to impose.

Information stored in the form of exograms accessible through sensory systems would be subject to many of the same issues surrounding **integrity**, **utility**, **availability**, **confidentiality**, **authenticity**, and **possession** that currently apply, for example, to information that a user might store on a mobile device and access through earphones or a virtual reality headset. If a neuroprosthetic device can be used to forcibly present information or activate the use of skills against the user's will, then questions of **autonomy** and **rejectability** also arise.

Functional impairments created by a neuroprosthetic device

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host at the level of his or her physical or virtual bodily interfaces with the environments and the impact that these impairments might have on the information security of the host-device system.[79]

Loss of control over sensory organs

A neuroprosthetic may deny its host or user direct control over his or her sensory organs.[80] Technologically mediated sensory systems may be subject

[79] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[80] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

to noise, malfunctions, and manipulation or forced sensory deprivation or overload occurring at the hands of sense hackers.[81]

A neuroprosthetic device that intentionally deprives its host or user of control over his or her sensory organs raises questions of the **rejectability** of sense data and may impair the host or user's exercise of agency and thus his or her **autonomy**. The **availability**, **integrity**, **utility**, and **authenticity** of information provided by the host or user's sensory organs will depend on the technical capacities and motives of whatever external agents control the design or operation of the neuroprosthetic device.

Loss of control over motor organs

A neuroprosthetic device may impede its host or user's control over his or her motor organs.[82] The host or user's body may no longer be capable, e.g., of speech or movement, or the control over one's speech or movements may be assumed by some external agency.

A neuroprosthetic device that intentionally deprives its host or user of control over his or her motor organs may prevent that person from inadvertently (or even purposefully) disclosing information through the use of speech, facial expressions, typing, or other physical means, thereby enhancing the **confidentiality** and **possession** of information.

The use of such a device may impair the information security of outside parties who, for example, interact with the host in conversation, listen to the host giving a lecture, or read a message that was typed and sent by the host: such individuals might assume that the information was conveyed to them intentionally by the host, while in fact it might have been conveyed against the host's will by some external agent who was controlling the host's motor activity through the neuroprosthetic device. This would result in a loss of **authenticity** of the information shared by the "host," from the perspective of those who received it.

Loss of control over other bodily systems

A neuroprosthetic device may impact the functioning of internal bodily processes such as respiration, cardiac activity, digestion, hormonal activity,

---

of Bionic Ears and Eyes" (2012), p. 130.

[81] Hansen and Hansen discuss the hypothetical case of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights. See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

[82] Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 216.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

and other processes that are already affected by existing implantable medical devices.[83]

Insofar as a neuroprosthetic device interfaces directly with such biological systems and processes, it may gather, store, utilize, and transmit data about them that must be secured in order to avoid a loss of **confidentiality** and **possession** of the information. By affecting the body's basic biological processes, a device may impact the brain's ability to receive, generate, store, transmit, and consciously experience information and may thus indirectly affect the **availability** and **utility** of information available to the host or user's mind.

Other biological side-effects

A neuroprosthetic device may be constructed from components that are toxic or deteriorate in the body,[84] may be rejected by its host, or may be subject to mechanical, electronic, or software failures that harm their host's organism.

Depending on the nature and severity of such effects, negative impacts could result for a host's **autonomy** and the **rejectability**, **integrity**, **utility**, **availability**, **authenticity**, and **distinguishability** of information experienced by a host or user.

On the other hand, if an advanced neuroprosthetic device is only able to function for a limited period of time before its connection to the neural circuitry of its host breaks down and the device ceases to function, this behavior could function as a sort of safeguard that limits the long-term possibilities for the device to contribute to a loss of the **confidentiality** or **possession** of information.

The host as social and economic actor

Functional capacities created by a neuroprosthetic device

Below we describe some of the new functional capacities that a neuroprosthetic device might provide to allow its host or user to connect to, participate in, contribute to, and be influenced by social relationships and structures and networks of economic exchange, and we note the potential impact that these capacities might have on the information security of the host-device system.[85]

---

[83] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 209, and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), pp. 12-16.

[84] McGee, "Bioelectronics and Implanted Devices" (2008), pp. 213-16.

[85] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

*Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.*

Ability to participate in new kinds of social relations

A neuroprosthetic device may grant its host or user the ability to participate in new kinds of technologically mediated social relations and structures that were previously impossible, perhaps including new forms of merged agency[86] or cybernetic networks that display utopian (or dystopian) characteristics that are not possible for non-neuroprosthetically-enabled societies.[87]

The creation of new kinds of social relationships may create new avenues for a host or user to inadvertently disclose information, thereby damaging its **confidentiality** and his or her **possession** of it. It may also provide new means for external agents to disrupt or influence the host or user's acquisition and use of information, not through manipulation of the device's components or systems but by using the device in its intended fashion to interact socially with its user and undermining the user's information security use through the nature and contents of those social interactions (which might involve social engineering[88]). This could indirectly impact the **availability** and **utility** of information for the user and may also potentially undermine his or her agency and thus **autonomy**.

Ability to share collective knowledge, skills, and wisdom

Neuroprosthetics may link hosts or users in a way that forms communication and information systems[89] that can generate greater collective knowledge, skills, and wisdom than are possessed by any individual member of the system.[90]

On the one hand, using a neuroprosthetic device to store information in communal systems that make their contents freely accessible to other human minds clearly eliminates the user's ability to maintain the **confidentiality** and

---

[86] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 216, and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 125, 132.

[87] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

[88] See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307-23; Sasse et al., "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security" (2001); and Thonnard, "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat" (2012).

[89] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 214; Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 128-29; Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 24; and Gladden, "'Upgrading' the Human Entity..." (2015).

[90] See Wiener, *Cybernetics* (1961), loc. 3070ff., 3149ff., and Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

possession of that information. On the other hand, by drawing information from "open-source" repositories whose maintenance and editing are crowdsourced to myriad minds that are continuously identifying and rectifying errors and which provide checks and balances to counteract one another's biases, it may be possible for such "neuroprosthetically enabled wikis" to maintain a self-healing and self-correcting state that offers greater **availability**, **integrity**, and **utility** of information than that possible from a static source developed by a single author.

Enhanced job flexibility and instant retraining

By facilitating the creation, alteration, and deletion of information stored in engrams or exograms, a neuroprosthetic device may allow its user to download new knowledge or skills or instantly establish relationships for use in a new job.[91]

A neuroprosthetic device that allows its user to enhance his or her socioeconomic position by continuously improving his or her skills, enhancing his or her job performance, and moving into ever more desirable and rewarding professions and positions may provide the user with resources (including financial, informational, and human resources and access to new technologies embodied in hardware, software, and services) that allow him or her to enhance and strengthen his or her information security, including his or her **autonomy**, the **confidentiality** and **possession** of information already in his or her control, the **availability** of new kinds of information, and enhanced tools for extracting **utility** from information.

Enhanced ability to manage complex technological systems

By providing a direct interface to external computers and mediating its user's interaction with them,[92] a neuroprosthetic device may grant an enhanced ability to manage complex technological systems that can be used, for example, for the production or provisioning of goods or services or the management of digital ecosystems and environments that utilize ubiquitous computing and are integrated into the Internet of Things.[93]

By giving the user of a neuroprosthetic device enhanced capacities for acquiring and managing information and controlling his or her environment, the device may offer the user increased **availability**, **utility**, **confidentiality**, **possession**, and **rejectability** of information.

---

[91] See Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 126, and Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[92] McGee, "Bioelectronics and Implanted Devices" (2008), p. 210.

[93] See McGee, "Bioelectronics and Implanted Devices" (2008), pp. 214-15, and Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics..." (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Enhanced personal and professional decision-making

By analyzing data, offering recommendations, and alerting the user to potential cognitive biases, a neuroprosthetic device may enhance its user's ability to execute rapid and effective personal and professional decision-making and transactions.[94]

By enhancing its user's ability to avoid the effects of internal biases and to identify and counteract intentional or inadvertent efforts by others to manipulate the user through social interaction, such a neuroprosthetic device may enhance its user's agency and **autonomy** and help prevent the user from inadvertently making decisions or undertaking actions that would undermine the **confidentiality** or **possession** of the user's information. It may also lead the user to make decisions which will eventually put the user in a position in which he or she enjoys greater **availability** and **utility** of information.

Store of monetary value

By storing cryptocurrency keys within its internal memory, a neuroprosthetic may allow its host to house digital money directly within his or her brain that can be spent on demand by the host.[95]

The use of a neuroprosthetic device to store information that has direct monetary value – rather than simply confidential personal or professional information which an unauthorized party might steal and attempt to convert into money through its sale or through blackmail of the host – creates an enticing new target for criminals and a new kind of information that must be carefully secured. For many users, the **possession** and **confidentiality** of such financial information would take priority and must be safeguarded, even if it means reducing the **availability** and **utility** of the information to the user.

A neuroprosthetic device that can be used directly to purchase goods and services and engage in other forms of economic exchange may give its user new tools for acquiring, utilizing, and securing information, thereby increasing the **availability** and **utility** of information as well as its **confidentiality** and **possession**.

---

[94] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 119.

[95] See Gladden, "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values" (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Qualifications for specific professions and roles

Neuroprosthetics may provide persons with abilities that enhance job performance in particular fields[96] such as computer programming, art, architecture, music, economics, medicine, information science, e-sports, information security, law enforcement, and the military. This may initially provide a competitive advantage to individuals using certain kinds of neuroprosthetic devices, while not excluding from such work those who lack neuroprosthetic devices. However, it is expected that as the use of elective neuroprosthetics becomes more commonplace and employers' expectations for employees' neural integration into digital workplace systems grow, possession of neuroprosthetics may become a basic requirement for employment in some professions that excludes from consideration potential workers who do not possess such devices.[97]

Insofar as individuals' use of advanced neuroprosthetic devices is a necessary and important aspect of their professional work, it can be expected that such employees' workplaces and employers will create and maintain robust institutional support systems for the users of such devices, which may include the attention of information security professionals dedicated to securing the information contained in these device-host systems. Such support structures may provide employees with stronger mechanisms for ensuring the **availability**, **utility**, **integrity**, **confidentiality**, and **possession** of information than they could obtain on their own if they acquired and utilized their neuroprosthetic devices solely in a role as ordinary consumers and personal, non-institutional users of such devices.

On the other hand, by allowing their employers to exercise at least some of the responsibility for maintaining, managing, and securing their neuroprosthetic devices, such users might instead find that an employer claims and acquires access to a user's personal information that is produced or accessible through the neuroprosthetic device, thereby reducing the **confidentiality** and **possession** of information by the user and potentially raising questions for the user about the extent to which the information's **availability**, **integrity**, and **authenticity** can be relied upon.

Functional impairments created by a neuroprosthetic device

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host or user at the level of his or her social

---

[96] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 131-32.

[97] McGee, "Bioelectronics and Implanted Devices" (2008), pp. 211, 214-15; Warwick, "The cyborg revolution" (2014), p. 269.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

and economic relationships and activity and the impact that these impairments might have on the information security of the host-device system.[98]

Loss of ownership of one's body and intellectual property

A neuroprosthetic device that is being leased by its human host rather than having been purchased would not belong to the host. Moreover, even a neuroprosthetic device that has been purchased by its host could potentially be subject to seizure by an outside party in some circumstances (e.g., after a declaration of bankruptcy by the host). Depending on the leasing or licensing terms, intellectual property produced by a neuroprosthetic device's host or user (including thoughts, memories, or speech) may be partly or wholly owned by the device's manufacturer or provider.[99]

This may result in binding limits on the **confidentiality**, **possession**, **availability**, and **utility** of information that can be enforced by the device's manufacturer or provider through either legal or technical means. The manufacturer or provider may also have the legal right and technical ability to forcibly present to the user's conscious or subconscious awareness explicit advertisements, product placements edited into the user's sense data, or other commercial information that undermines the **rejectability** and perhaps **distinguishability** and **authenticity** of information received through the device. The fine print of the leasing, licensing, or even purchase agreement may also specify that the device's manufacturer or provider has the legal right to utilize the device to gather on an ongoing basis information about its host or user (including information about his or her biological and mental processes), which the company can either use internally for its own purposes or perhaps rent or sell to other companies for their own uses. This would have the effect of significantly reducing the **confidentiality** and **possession** of personal information by the host or user.

On the other hand, by maintaining an ongoing financial relationship with the device's manufacturer or provider, the user may be able to make use of physical maintenance services, software updates and upgrades (including regular updating of antivirus and other security software), and other services provided by that firm which enhances the **confidentiality**, **possession**, **availability**, **utility**, and **integrity** of information experienced through the device.

---

[98] See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

[99] See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Creation of financial, technological, or social dependencies

The host or user of a neuroprosthetic may no longer be able to function effectively without the device[100] and may become dependent on its manufacturer for hardware maintenance, software updates, and data security and on specialized medical care providers for diagnostics and treatment relating to the device.[101] A user may also require regular device upgrades in order to remain competitive in certain jobs for which the possession and expert use of such a device is a job requirement. High switching costs may make it impractical to shift to a competing producer's device after a host has installed an implant and committed to its manufacturer's particular digital ecosystem.

If the host or user of a neuroprosthetic device is likely to suffer biological, psychological, financial, professional, or social damage without such ongoing specialized support from a company, this creates a power relation in which the host or user is in a position of dependency (or even subjugation) and in which he or she may be willing to accept an exploitative situation in which the **confidentiality** and **possession** of his or her information is compromised by the company, his or her autonomy is diminished, and the **availability**, **utility**, **integrity**, and **rejectability** of information is subject to the whims (likely driven by financial considerations) of the company.

Subjugation of the host to manipulation by external agency

Instead of merely impeding its host or user's ability to possess and exercise agency, a neuroprosthetic may subject its host to control by some external agency. This could occur, e.g., if the host's memories, emotions, or volitions were manipulated by means of the device[102] or if the host joined with other minds to create a new form of social entity that possesses some shared agency.[103]

---

[100] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 125.

[101] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 213. Brain scarring is a significant problem with neuroprosthetic devices involving electrodes implanted in the brain, and the administration before, during, and after implantation surgery of immunosuppressive drugs that reduce the wound healing response has been found to reduce scarring and cortical edemas; see See Polikov et al., "Response of brain tissue to chronically implanted neural electrodes" (2005), for a discussion of such issues. The possibility that the host of an implanted advanced neuroprosthetic device might become dependent throughout the rest of his or her life on the device's manufacturer (or another commercial entity) for a regular supply of potentially expensive and proprietary immunosuppressive drugs or other specialized medications is a theme that has been explored by futurologists and the creators of science fiction works; for an analysis of a prime fictional depiction, see Maj, "Rational Technotopia vs. Corporational Dystopia in 'Deus Ex: Human Revolution' Gameworld" (2015).

[102] Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), pp. 15-16.

[103] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 216, and Gladden, "'Upgrading'

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Such a situation would impair the host's **autonomy** and could be exploited to undermine the **confidentiality** and **possession** of the host's information. Depending on the level of access to the host's information that is gained by the external agent, the **authenticity**, **integrity**, **availability**, and **utility** of the host's information could also be imperiled.

Social exclusion and fragmentation and employment discrimination

The use of particular kinds of neuroprosthetics that are considered by a particular society to be of a "suspicious" or "undesirable" nature and whose presence and operation is detectable to parties other than their host or user may result in the shunning or mistreatment of such hosts or users[104] by those who question or actively oppose the use of such devices.[105] Hosts or users of such neuroprosthetic devices may find themselves formally or informally excluded from certain kinds of organizations and social relationships, or they may simply avoid certain kinds of relationships and situations in order to spare themselves the embarrassment or discomfort that might result from such interactions. Possession of some kinds of neuroprosthetics may exclude their hosts from employment in roles where "natural," unmodified workers are considered desirable or even required (e.g., for liability or security reasons).

It is also expected that some kinds of advanced neuroprosthetics will so radically transform their users' channels for communicating and interacting socially that they will eventually lose the desire and even ability to communicate with human beings who do not possess the relevant sort of neuroprosthetics; in this way, humanity as it exists today may fragment into numerous mutually incomprehensible "posthumanities" that share a geographical home on this planet but whose societies and civilizations occupy disjoint psychological, cultural, and technological spaces that do not intersect or overlap.[106]

---

the Human Entity..." (2015).

[104] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 124-25.

[105] For example, anecdotal accounts have already been reported of physical harassment and exclusion from places of business of individuals wearing external sensory prosthetics designed to generate visual augmented reality. See Greenberg, "Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out" (2012), and Dvorsky, "What may be the world's first cybernetic hate crime unfolds in French McDonald's" (2012).

[106] See McGee, "Bioelectronics and Implanted Devices" (2008), pp. 214-16; Warwick, "The cyborg revolution" (2014), p. 271; and Rubin, "What Is the Good of Transhumanism?" (2008).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Such a splintering and narrowing of societies may possibly weaken the solidarity with other human beings exhibited by users of some kinds of advanced neuroprosthetics.[107]

If the users of certain kinds of neuroprosthetics were, in essence, to withdraw from "normal" human society and develop new societies accessible only to those who share similar technological augmentation, interests, and philosophies, one side-effect of this growing distance and insulation from human society could be an increase in the **confidentiality** and **possession** of information by the users of such technologies, insofar as the ability of unaugmented humans to initiate some kinds of attacks (such as social engineering efforts) might be significantly curtailed. At the same time, the users of such neuroprosthetic devices might find that their voluntary or involuntary distancing from the rest of humanity separates them legally, politically, commercially, socially, or technologically from information security systems and mechanisms that are available to other human beings, thereby potentially putting at risk the **integrity**, **availability**, **confidentiality**, and **possession** of the users' information.

Vulnerability to data theft, blackmail, and extortion

A hacker, computer virus, or other agent may be able to steal data contained in a neuroprosthetic device or use the device to gather data (potentially including the contents of thoughts, memories, or sensory experiences)[108] that could be used for blackmail, extortion, corporate espionage, or terrorism targeted against the device's host or user or other individuals or institutions. Such an attacker could either carry out a one-time theft of information or embed in the device software (or even hardware) that allows ongoing access and the ability to utilize the device's features and components as an instrument for information-gathering and surveillance, regardless of whether they were designed to be employable for such purposes.

The minds, personalities, interests, motivations, and values of all human beings are different, which means that the authors of certain kinds of social engineering attacks on high-value targets must take the time to learn about the subject of their intended operation and develop a customized plan of attack, and it cannot be known for certain in advance of the attack whether or not it will succeed and what unexpected obstacles might arise during its attempted execution.[109] If the target of such an attack possesses an advanced

---

[107] Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 127.

[108] See McGee, "Bioelectronics and Implanted Devices" (2008), p. 217; Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 117, 130; and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 21.

[109] See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307-23, and Sasse et al., "Transforming

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

neuroprosthetic device, this may give the attacker a means of planning and executing the attack that depends solely on technical and technological factors (which it may be possible to analyze carefully in advance) rather than social and psychological ones. Exploitable vulnerabilities in a particular model of neuroprosthetic device that have been identified by would-be attackers may place at risk all human beings who possess that particular model of device, regardless of the otherwise great psychological, cultural, and professional dissimilarities between them.

Depending on the exact purpose and nature of such an attack, it may have the potential to undermine the **confidentiality** and **possession** both of the host or user's information and the information of other parties that can be compromised by means of the neuroprosthetic device (e.g., by using a neuroprosthetic device implanted in one person to eavesdrop on a separate individual who happens to be nearby). It may also compromise the **authenticity**, **integrity**, **availability**, **distinguishability**, and **utility** of information and be employed to undermine the host or user's **autonomy**.

Conclusion

In this chapter we have explored a two-dimensional conceptual framework for cognitional security that comprises nine essential information security goals for neuroprosthetic devices and device-host systems (confidentiality, integrity, availability, possession, authenticity, utility, distinguishability, rejectability, and autonomy) and examines potential impacts on the pursuit of those goals as observed at three different levels (which consider a device's host understood as sapient metavolitional agent, embodied embedded organism, and social and economic actor). In the following chapters we will draw on this cognitional security framework to consider important practical issues relating to the development and implementation of information security plans for advanced neuroprosthetics – namely, the formulation of particular information security roles and responsibilities and the design and use of management, operational, and technical controls.

---

the 'weakest link'—a human/computer interaction approach to usable and effective security" (2001).

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Bibliography

Abrams, Jerold J. "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault." *Human Studies* 27, no. 3 (September 1, 2004): 241-58. doi:10.1023/B:HUMA.0000042130.79208.c6.

Al-Hudhud, Ghada. "On Swarming Medical Nanorobots." *International Journal of Bio-Science & Bio-Technology* 4, no. 1 (March 2012): 75-90.

Ameen, Moshaddique Al, Jingwei Liu, and Kyungsup Kwak. "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications." *Journal of Medical Systems* 36, no. 1 (March 12, 2010): 93-101. doi:10.1007/s10916-010-9449-4.

Ankarali, Z.E., Q.H. Abbasi, A.F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan. "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security." In *2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)*, 246-49, 2014. doi:10.1109/MOBIHEALTH.2014.7015957.

Ansari, Sohail, K. Chaudhri, and K. Al Moutaery. "Vagus Nerve Stimulation: Indications and Limitations." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 281-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Armando, Alessandro, Gabriele Costa, Alessio Merlo, and Luca Verderame. "Formal Modeling and Automatic Enforcement of Bring Your Own Device Policies." *International Journal of Information Security*, (August 10, 2014): 1-18. doi:10.1007/s10207-014-0252-y.

Ayaz, Hasan, Patricia A. Shewokis, Scott Bunce, Maria Schultheis, and Banu Onaral. "Assessment of Cognitive Neural Correlates for a Functional Near Infrared-Based Brain Computer Interface System." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 699-708. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Baars, Bernard J. *In the Theater of Consciousness.* New York, NY: Oxford University Press, 1997.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Baddeley, Alan. "The episodic buffer: a new component of working memory?" *Trends in cognitive sciences* 4, no. 11 (2000): 417-423.

Baudrillard, Jean. *Simulacra and Simulation*. Ann Arbor: University of Michigan Press, 1994.

Berg, Bibi van den. "Pieces of Me: On Identity and Information and Communications Technology Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 159-73. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Bergamasco, S., M. Bon, and P. Inchingolo. "Medical data protection with a new generation of hardware authentication tokens." In *IFMBE Proceedings MEDICON 2001*, edited by R. Magjarevic, S. Tonkovic, V. Bilas, and I. Lackovic, 82-85. IFMBE, 2001.

Birbaumer, Niels, and Klaus Haagen. "Restoration of Movement and Thought from Neuroelectric and Metabolic Brain Activity: Brain-Computer Interfaces (BCIs)." In *Intelligent Computing Everywhere*, edited by Dr Alfons J. Schuster, 129-52. Springer London, 2007.

Birnbacher, Dieter. "Posthumanity, Transhumanism and Human Nature." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 95-106. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Borkar, Shekhar. "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation." *Micro, IEEE* 25, no. 6 (2005): 10-16.

Borton, D. A., Y.-K. Song, W. R. Patterson, C. W. Bull, S. Park, F. Laiwalla, J. P. Donoghue, and A. V. Nurmikko. "Implantable Wireless Cortical Recording Device for Primates." In *World Congress on Medical Physics and Biomedical Engineering, September 7-12, 2009, Munich, Germany*, edited by Olaf Dössel and Wolfgang C. Schlegel, 384-87. IFMBE Proceedings 25/9. Springer Berlin Heidelberg, 2009.

Bostrom, Nick. "Why I Want to Be a Posthuman When I Grow Up." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 107-36. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Bowman, Diana M., Mark N. Gasson, and Eleni Kosta. "The Societal Reality of That Which Was Once Science Fiction." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 175-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Braddon-Mitchell, David, and John Fitzpatrick. "Explanation and the Language of Thought." *Synthese* 83, no. 1 (April 1, 1990): 3-29. doi:10.1007/BF00413686.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Bradshaw, Jeffrey M., Paul Feltovich, Matthew Johnson, Maggie Breedy, Larry Bunch, Tom Eskridge, Hyuckchul Jung, James Lott, Andrzej Uszok, and Jurriaan van Diggelen. "From Tools to Teammates: Joint Activity in Human-Agent-Robot Teams." In *Human Centered Design*, edited by Masaaki Kurosu, 935-44. Lecture Notes in Computer Science 5619. Springer Berlin Heidelberg, 2009.

Brey, Philip. "Ethical Aspects of Information Security and Privacy." In *Security, Privacy, and Trust in Modern Data Management*, edited by Milan Petković and Willem Jonker, 21-36. Data-Centric Systems and Applications. Springer Berlin Heidelberg, 2007.

Brunner, Peter, and Gerwin Schalk. "Brain-Computer Interaction." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 719-23. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Buller, Tom. "Neurotechnology, Invasiveness and the Extended Mind." *Neuroethics* 6, no. 3 (August 18, 2011): 593-605. doi:10.1007/s12152-011-9133-5.

Calverley, D.J. "Imagining a non-biological machine as a legal person." *AI & SOCIETY* 22, no. 4 (2008): 523-37.

Campbell, Courtney S., James F. Keenan, David R. Loy, Kathleen Matthews, Terry Winograd, and Laurie Zoloth. "The Machine in the Body: Ethical and Religious Issues in the Bodily Incorporation of Mechanical Devices." In *Altering Nature*, edited by B. Andrew Lustig, Baruch A. Brody, and Gerald P. McKenny, 199-257. Philosophy and Medicine 98. Springer Netherlands, 2008.

Cavallari, Maurizio. "Organisational Constraints on Information Systems Security." In *Emerging Themes in Information Systems and Organization Studies*, edited by Andrea Carugati and Cecilia Rossignoli, 193-207. Physica-Verlag HD, 2011.

Cervera-Paz, Francisco Javier, and M. J. Manrique. "Auditory Brainstem Implants: Past, Present and Future Prospects." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 437-42. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Chadwick, Ruth. "Therapy, Enhancement and Improvement." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 25-37. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Chaudhry, Peggy E., Sohail S. Chaudhry, Ronald Reese, and Darryl S. Jones. "Enterprise Information Systems Security: A Conceptual Framework." In *Re-Conceptualizing Enterprise Information Systems*, edited by Charles Møller

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

and Sohail Chaudhry, 118-28. Lecture Notes in Business Information Processing 105. Springer Berlin Heidelberg, 2012.

Cho, Kwantae, and Dong Hoon Lee. "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks." In *Information Security Applications*, edited by Souhwan Jung and Moti Yung, 203-18. Lecture Notes in Computer Science 7115. Springer Berlin Heidelberg, 2012.

Church, George M., Yuan Gao, and Sriram Kosuri. "Next-generation digital information storage in DNA." *Science* 337, no. 6102 (2012): 1628.

Clark, Andy. "Systematicity, Structured Representations and Cognitive Architecture: A Reply to Fodor and Pylyshyn." In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 198-218. Studies in Cognitive Systems 9. Springer Netherlands, 1991.

Clark, S.S., and K. Fu, "Recent Results in Computer Security for Medical Devices," in *Wireless Mobile Communication and Healthcare*, edited by K.S. Nikita, J.C. Lin, D.I. Fotiadis, and M.-T. Arredondo Waldmeyer, 111-18. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 83. Springer Berlin Heidelberg, 2012.

Claussen, Jens Christian, and Ulrich G. Hofmann. "Sleep, Neuroengineering and Dynamics." *Cognitive Neurodynamics* 6, no. 3 (May 27, 2012): 211-14. doi:10.1007/s11571-012-9204-2.

Clowes, Robert W. "The Cognitive Integration of E-Memory." *Review of Philosophy and Psychology* 4, no. 1 (January 26, 2013): 107-33. doi:10.1007/s13164-013-0130-y.

Coeckelbergh, M. "From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots." *Philosophy & Technology* 24, no. 3 (2011): 269-78.

Coles-Kemp, Lizzie, and Marianthi Theoharidou. "Insider Threat and Information Security Management." In *Insider Threats in Cyber Security*, edited by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, 45-71. Advances in Information Security 49. Springer US, 2010.

Cory, Jr., Gerald A. "Language, Brain, and Neuron." In *Toward Consilience*, 193-205. Springer US, 2000.

Cosgrove, G.R. (2004). "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation." Meeting of the President's Council on Bioethics. Washington, DC, June 24-25, 2004. https://bioethicsarchive.georgetown.edu/pcbe/transcripts/june04/session6.html. Accessed June 12, 2015.

Dardick, Glenn. "Cyber Forensics Assurance." In *Proceedings of the 8th Australian Digital Forensics Conference*, 57-64. Research Online, 2010.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Datteri, E. "Predicting the Long-Term Effects of Human-Robot Interaction: A Reflection on Responsibility in Medical Robotics." *Science and Engineering Ethics* 19, no. 1 (2013): 139-60.

Delac, Kresimir, and Mislav Grgic. "A Survey of Biometric Recognition Methods." In *Proceedings of the 46th International Symposium on Electronics in Marine, ELMAR 2004*, 184-93. IEEE, 2004.

Denning, Tamara, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H. Maisel. "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 917-26. ACM, 2010.

Denning, Tamara, Kevin Fu, and Tadayoshi Kohno. "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security." 3rd USENIX Workshop on Hot Topics in Security (HotSec 2008). San Jose, CA, July 29, 2008.

Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. "Neurosecurity: Security and Privacy for Neural Devices." *Neurosurgical Focus* 27, no. 1 (2009): E7. doi:10.3171/2009.4.FOCUS0985.

Donchin, Emanuel, and Yael Arbel. "P300 Based Brain Computer Interfaces: A Progress Report." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 724-31. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Drongelen, Wim van, Hyong C. Lee, and Kurt E. Hecox. "Seizure Prediction in Epilepsy." In *Neural Engineering*, edited by Bin He, 389-419. Bioelectric Engineering. Springer US, 2005.

Dudai, Yadin. "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" *Annual Review of Psychology* 55 (2004): 51-86. doi:10.1146/annurev.psych.55.090902.142050.

Durand, Dominique M., Warren M. Grill, and Robert Kirsch. "Electrical Stimulation of the Neuromuscular System." In *Neural Engineering*, edited by Bin He, 157-91. Bioelectric Engineering. Springer US, 2005.

Dvorsky, George. "What may be the world's first cybernetic hate crime unfolds in French McDonald's." io9, July 17, 2012. http://io9.com/5926587/what-may-be-the-worlds-first-cybernetic-hate-crime-unfolds-in-french-mcdonalds. Accessed July 22, 2015.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Edgar, Andrew. "The Hermeneutic Challenge of Genetic Engineering: Habermas and the Transhumanists." *Medicine, Health Care and Philosophy* 12, no. 2 (May 1, 2009): 157-67. doi:10.1007/s11019-009-9188-9.

Edlinger, Günter, Cristiano Rizzo, and Christoph Guger. "Brain Computer Interface." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1003-17. Springer Berlin Heidelberg, 2011. http://link.springer.com/chapter/10.1007/978-3-540-74658-4_52.

Erler, Alexandre. "Does Memory Modification Threaten Our Authenticity?" *Neuroethics* 4, no. 3 (November 2011): 235-49. doi:10.1007/s12152-010-9090-4.

Fairclough, S.H. "Physiological Computing: Interfacing with the Human Nervous System." In *Sensing Emotions*, edited by J. Westerink, M. Krans, and M. Ouwerkerk ,1-20. Philips Research Book Series 12. Springer Netherlands, 2010.

Fernandes, Diogo A. B., Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio. "Security Issues in Cloud Environments: A Survey." *International Journal of Information Security* 13, no. 2 (September 28, 2013): 113-70. doi:10.1007/s10207-013-0208-7.

Fernandez-Lopez, Helena, José A. Afonso, J. H. Correia, and Ricardo Simoes. "The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems." In *Sensor Systems and Software*, edited by Francisco Martins, Luís Lopes, and Hervé Paulino, 137-45. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 102. Springer Berlin Heidelberg, 2012.

Ferrando, Francesca. "Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations." *Existenz: An International Journal in Philosophy, Religion, Politics, and the Arts* 8, no. 2 (Fall 2013): 26-32.

"FIPA Device Ontology Specification." Foundation for Intelligent Physical Agents (FIPA), May 10, 2002. http://www.fipa.org/assets/XC00091D.pdf. Accessed February 9, 2015.

Fleischmann, Kenneth R. "Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI." *The Information Society* 25, no. 4 (2009): 227-35. doi:10.1080/01972240903028359.

Flemisch, F., M. Heesen, T. Hesse, J. Kelsch, A. Schieben, and J. Beller. "Towards a Dynamic Balance between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations." *Cognition, Technology & Work* 14, no. 1 (2012): 3-18. doi:10.1007/s10111-011-0191-6.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Fountas, Kostas N., and J. R. Smith. "A Novel Closed-Loop Stimulation System in the Control of Focal, Medically Refractory Epilepsy." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 357-62. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Fox, S. and L. Rainie. "The Web at 25 in the US: Part 1: How the Internet Has Woven Itself into American Life." Pew Research Center's Internet & American Life Project, February 27, 2014. http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/. Accessed July 24, 2015.

Freudenthal, Eric, Ryan Spring, and Leonardo Estevez. "Practical techniques for limiting disclosure of RF-equipped medical devices." In *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*, 82-85. IEEE, 2007.

Friedenberg, Jay. *Artificial Psychology: The Quest for What It Means to Be Human*, Philadelphia: Psychology Press, 2011.

Gärtner, Armin. "Communicating Medical Systems and Networks." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1085-93. Springer Berlin Heidelberg, 2011.

Gasson, M.N., Kosta, E., and Bowman, D.M. "Human ICT Implants: From Invasive to Pervasive." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 1-8. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Gasson, M.N. "Human ICT Implants: From Restorative Application to Human Enhancement." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 11-28. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Gasson, M.N. "ICT implants." In *The Future of Identity in the Information Society*, edited by S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, 287-95. Springer US, 2008.

Gerhardt, Greg A., and Patrick A. Tresco. "Sensor Technology." In *Brain-Computer Interfaces*, 7-29. Springer Netherlands, 2008.

Gladden, Matthew E. "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values." Ethics in Economic Life. Uniwersytet Łódzki, Łódź, May 8, 2015.

Gladden, Matthew E. "Cybershells, Shapeshifting, and Neuroprosthetics: Video Games as Tools for Posthuman 'Body Schema (Re)Engineering'." Ogólnopolska Konferencja Naukowa Dyskursy Gier Wideo. Facta Ficta, AGH, Kraków, June 6, 2015.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Gladden, Matthew E. "A Fractal Measure for Comparing the Work Effort of Human and Artificial Agents Performing Management Functions." In *Position Papers of the 2014 Federated Conference on Computer Science and Information Systems*, edited by Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki, 219-26. Annals of Computer Science and Information Systems 3. Polskie Towarzystwo Informatyczne, 2014.

Gladden, Matthew E. "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Gladden, Matthew E. "The Social Robot as 'Charismatic Leader': A Phenomenology of Human Submission to Nonhuman Power." In *Sociable Robots and the Future of Social Relations: Proceedings of Robo-Philosophy 2014*, edited by Johanna Seibt, Raul Hakli, and Marco Nørskov, 329-39. Frontiers in Artificial Intelligence and Applications 273. IOS Press, 2014.

Gladden, Matthew E. "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences." His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta, Jagiellonian University, Kraków, March 24, 2015.

Gladden, Matthew E. "'Upgrading' the Human Entity: Cyberization as a Path to Posthuman Utopia or Digital Annihilation?" Arkana Fantastyki lecture cycle. Centrum Informacji Naukowej i Biblioteka Akademicka (CINiBA), Katowice, May 27, 2015.

Gordijn, Bert. "Converging NBIC Technologies for Improving Human Performance." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 225-35. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Greenberg, Andy. "Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out." Forbes, July 17, 2012. http://www.forbes.com/sites/andygreenberg/2012/07/17/cyborg-discrimination-scientist-says-mcdonalds-staff-tried-to-pull-off-his-google-glass-like-eyepiece-then-threw-him-out/. Accessed July 22, 2015.

Grodzinsky, F.S., K.W. Miller, and M.J. Wolf. "Developing Artificial Agents Worthy of Trust: 'Would You Buy a Used Car from This Artificial Agent?'" *Ethics and Information Technology* 13, no. 1 (2011): 17-27.

Grottke, M., H. Sun, R. M. Fricks, and K. S. Trivedi. "Ten fallacies of availability and reliability analysis." In *Service Availability*, 187-206. Lecture Notes in Computer Science 5017. Springer Berlin Heidelberg, 2008. http://dx.doi.org/10.1007/978-3-540-68129-8_15.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Gunkel, David, and Debra Hawhee. "Virtual Alterity and the Reformatting of Ethics." *Journal of Mass Media Ethics* 18, no. 3-4 (2003): 173-93. doi:10.1080/08900523.2003.9679663.

Gunther, N. J. "Time—the zeroth performance metric." In *Analyzing Computer System Performance with Perl::PDQ*, 3-46. Berlin: Springer, 2005. http://dx.doi.org/10.1007/978-3-540-26860-4_1.

Halperin, Daniel, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." In *IEEE Symposium on Security and Privacy, 2008. SP 2008*, 129-142. IEEE, 2008.

Halperin, Daniel, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maisel. "Security and privacy for implantable medical devices." *Pervasive Computing, IEEE* 7, no. 1 (2008): 30-39.

Han, J.-H., S.A. Kushner, A.P. Yiu, H.-W. Hsiang, T. Buch, A. Waisman, B. Bontempi, R.L. Neve, P.W. Frankland, and S.A. Josselyn. "Selective Erasure of a Fear Memory." *Science* 323, no. 5920 (2009): 1492-96.

Hansen, Jeremy A., and Nicole M. Hansen. "A Taxonomy of Vulnerabilities in Implantable Medical Devices." In *Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems*, 13-20. ACM, 2010.

Hanson, R. (1994). "If uploads come first: The crack of a future dawn." *Extropy* 6, no. 2 (1994), 10-15.

Harrison, Ian. "IEC80001 and Future Ramifications for Health Systems Not Currently Classed as Medical Devices." In *Making Systems Safer*, edited by Chris Dale and Tom Anderson, 149-71. Springer London, 2010.

Hatfield, B., A. Haufler, and J. Contreras-Vidal. "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 810-17. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Hei, Xiali, and Xiaojiang Du. "Biometric-based two-level secure access control for implantable medical devices during emergencies." In *INFOCOM, 2011 Proceedings IEEE*, 346-350. IEEE, 2011.

Heersmink, Richard. "Embodied Tools, Cognitive Tools and Brain-Computer Interfaces." *Neuroethics* 6, no. 1 (September 1, 2011): 207-19. doi:10.1007/s12152-011-9136-2.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Hellström, T. "On the Moral Responsibility of Military Robots," *Ethics and Information Technology* 15, no. 2 (2013): 99-107.

Hern, Alex. "Hacker fakes German minister's fingerprints using photos of her hands." The Guardian, December 30, 2014. http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands. Accessed July 24, 2015.

Hildebrandt, Mireille, and Bernhard Anrig. "Ethical Implications of ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 135-58. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Hoffmann, Klaus-Peter, and Silvestro Micera. "Introduction to Neuroprosthetics." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 785-800. Springer Berlin Heidelberg, 2011.

Humphreys, L., J. M. Ferrández, and E. Fernández. "Long Term Modulation and Control of Neuronal Firing in Excitable Tissue Using Optogenetics." In *Foundations on Natural and Artificial Computation*, edited by José Manuel Ferrández, José Ramón Álvarez Sánchez, Félix de la Paz, and F. Javier Toledo, 266-73. Lecture Notes in Computer Science 6686. Springer Berlin Heidelberg, 2011.

Illes, Judy. Neuroethics: Defining the Issues in Theory, Practice, and Policy. Oxford University Press, 2006.

Josselyn, Sheena A. "Continuing the Search for the Engram: Examining the Mechanism of Fear Memories." *Journal of Psychiatry & Neuroscience : JPN* 35, no. 4 (July 2010): 221-28. doi:10.1503/jpn.100015.

Katz, Gregory. "The Hypothesis of a Genetic Protolanguage: An Epistemological Investigation." *Biosemiotics* 1, no. 1 (February 8, 2008): 57-73. doi:10.1007/s12304-008-9005-5.

Kirkpatrick, K. "Legal Issues with Robots." *Communications of the ACM* 56, no. 11 (2013): 17-19.

KleinOsowski, A., Ethan H. Cannon, Phil Oldiges, and Larry Wissel. "Circuit design and modeling for soft errors." *IBM Journal of Research and Development* 52, no. 3 (2008): 255-63.

Kłoda-Staniecko, Bartosz. "Ja, Cyborg. Trzy porządki, jeden byt. Podmiot jako fuzja biologii, kultury i technologii" ("I, Cyborg. Three Orders, One Being. Subject as a Fusion of Nature, Culture and Technology"). In *Człowiek w relacji do zwierząt, roślin i maszyn w kulturze: Tom I: Aspekt posthumanistyczny i transhumanistyczny*, edited by Justyny Tymienieckiej-Suchanek. Uniwersytet Śląski, 2015.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Koch, K. P. "Neural Prostheses and Biomedical Microsystems in Neurological Rehabilitation." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 427-34. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Koebler, Jason. "FCC Cracks Down on Cell Phone 'Jammers': The FCC says illegal devices that block cell phone signals could pose security risk." U.S. News & World Report, October 17, 2012. http://www.usnews.com/news/articles/2012/10/17/fcc-cracks-down-on-cell-phone-jammers. Accessed July 22, 2015.

Koene, Randal A. "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation." In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 241-67. The Frontiers Collection. Springer Berlin Heidelberg, 2012.

Kolkowska, Ella, and Gurpreet Dhillon. "Organizational Power and Information Security Rule Compliance." In *Future Challenges in Security and Privacy for Academia and Industry*, edited by Jan Camenisch, Simone Fischer-Hübner, Yuko Murayama, Armand Portmann, and Carlos Rieder, 185-96. IFIP Advances in Information and Communication Technology 354. Springer Berlin Heidelberg, 2011.

Koops, B.-J., and R. Leenes (2012). "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 113-34. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Kosta, E., and D.M. Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 97-112. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Kourany, J.A. (2013). "Human enhancement: Making the debate more Productive." *Erkenntnis* 79, no. 5 (2013): 981-98.

Kowalewska, Agata. "Symbionts and Parasites – Digital Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Kraemer, Felicitas. "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation." *Neuroethics* 6, no. 3 (May 12, 2011): 483-97. doi:10.1007/s12152-011-9115-7.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Kuflik, A. "Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?" *Ethics and Information Technology* 1, no. 3 (1999): 173-84.

Lebedev, M., "Brain-Machine Interfaces: An Overview," *Translational Neuroscience* 5, no. 1 (March 28, 2014): 99-110.

Leder, Felix, Tillmann Werner, and Peter Martini. "Proactive Botnet Countermeasures: An Offensive Approach." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 211-25. Cryptology and Information Security Series. IOS Press, 2009. doi:10.3233/978-1-60750-060-5-211.

Lee, Giljae, Andréa Matsunaga, Salvador Dura-Bernal, Wenjie Zhang, William W. Lytton, Joseph T. Francis, and José AB Fortes. "Towards Real-Time Communication between in Vivo Neurophysiological Data Sources and Simulator-Based Brain Biomimetic Models." *Journal of Computational Surgery* 3, no. 1 (November 11, 2014): 1-23. doi:10.1186/s40244-014-0012-3.

Li, S., F. Hu, and G. Li, "Advances and Challenges in Body Area Network." In *Applied Informatics and Communication*, edited by J. Zhan, 58-65. Communications in Computer and Information Science 22. Springer Berlin Heidelberg, 2011.

Linsenmeier, Robert A. "Retinal Bioengineering." In *Neural Engineering*, edited by Bin He, 421-84. Bioelectric Engineering. Springer US, 2005.

Lloyd, David. "Biological Time Is Fractal: Early Events Reverberate over a Life Time." *Journal of Biosciences* 33, no. 1 (March 1, 2008): 9–19. doi:10.1007/s12038-008-0017-8.

Longuet-Higgins, H.C. "Holographic Model of Temporal Recall." *Nature* 217, no. 5123 (1968): 104. doi:10.1038/217104a0.

Lorence, Daniel, Anusha Sivaramakrishnan, and Michael Richards. "Transaction-Neutral Implanted Data Collection Interface as EMR Driver: A Model for Emerging Distributed Medical Technologies." *Journal of Medical Systems* 34, no. 4 (March 20, 2009): 609-17. doi:10.1007/s10916-009-9274-9.

Lucivero, Federica, and Guglielmo Tamburrini. "Ethical Monitoring of Brain-Machine Interfaces." *AI & SOCIETY* 22, no. 3 (August 3, 2007): 449-60. doi:10.1007/s00146-007-0146-x.

Ma, Ting, Ying-Ying Gu, and Yuan-Ting Zhang. "Circuit Models for Neural Information Processing." In *Neural Engineering*, edited by Bin He, 333-65. Bioelectric Engineering. Springer US, 2005.

MacVittie, Kevin, Jan Halámek, Lenka Halámková, Mark Southcott, William D. Jemison, Robert Lobel, and Evgeny Katz. "From 'cyborg' lobsters to a pacemaker powered by implantable biofuel cells." *Energy & Environmental Science* 6, no. 1 (2013): 81-86.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Maj, Krzysztof. "Rational Technotopia vs. Corporational Dystopia in 'Deus Ex: Human Revolution' Gameworld." His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta, Jagiellonian University, Kraków, March 24, 2015.

Mak, Stephen. "Ethical Values for E-Society: Information, Security and Privacy." In *Ethics and Policy of Biometrics*, edited by Ajay Kumar and David Zhang, 96-101. Lecture Notes in Computer Science 6005. Springer Berlin Heidelberg, 2010.

Masani, Kei, and Milos R. Popovic. "Functional Electrical Stimulation in Rehabilitation and Neurorehabilitation." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 877-96. Springer Berlin Heidelberg, 2011.

McCormick, Michael. "Data Theft: A Prototypical Insider Threat." In *Insider Attack and Cyber Security*, edited by Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith, and Sara Sinclair, 53-68. Advances in Information Security 39. Springer US, 2008.

McCullagh, P., G. Lightbody, J. Zygierewicz, and W.G. Kernohan, "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology." *Neuroethics* 7, no. 2 (July 28, 2013): 109-22.

McGee, E.M., "Bioelectronics and Implanted Devices." In *Medical Enhancement and Posthumanity*, edited by B. Gordijn and R. Chadwick, 207-24. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

McGrath, Michael J., and Cliodhna Ní Scanaill. "Regulations and Standards: Considerations for Sensor Technologies." In *Sensor Technologies*, 115-35. Apress, 2013.

Meloy, Stuart. "Neurally Augmented Sexual Function." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 359-63. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Merkel, R., G. Boer, J. Fegert, T. Galert, D. Hartmann, B. Nuttin, and S. Rosahl, "Central Neural Prostheses." In *Intervening in the Brain: Changing Psyche and Society*, 117-60. Ethics of Science and Technology Assessment 29. Springer Berlin Heidelberg, 2007.

Miah, Andy. "A Critical History of Posthumanism." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 71-94. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Miller, Kai J., and Jeffrey G. Ojemann. "A Simple, Spectral-Change Based, Electrocorticographic Brain–Computer Interface." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 241-58. The Frontiers Collection. Springer Berlin Heidelberg, 2009.

Mitcheson, Paul D. "Energy harvesting for human wearable and implantable bio-sensors." In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE,* 3432-3436. IEEE, 2010.

Mizraji, Eduardo, Andrés Pomi, and Juan C. Valle-Lisboa. "Dynamic Searching in the Brain." *Cognitive Neurodynamics* 3, no. 4 (June 3, 2009): 401-14. doi:10.1007/s11571-009-9084-2.

Moravec, Hans. *Mind Children: The Future of Robot and Human Intelligence*. Cambridge: Harvard University Press, 1990.

Moxon, Karen A. "Neurorobotics." In *Neural Engineering*, edited by Bin He, 123-55. Bioelectric Engineering. Springer US, 2005.

Negoescu, R. "Conscience and Consciousness in Biomedical Engineering Science and Practice." In *International Conference on Advancements of Medicine and Health Care through Technology*, edited by Simona Vlad, Radu V. Ciupa, and Anca I. Nicu, 209-14. IFMBE Proceedings 26. Springer Berlin Heidelberg, 2009.

Neuper, Christa, and Gert Pfurtscheller. "Neurofeedback Training for BCI Control." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 65-78. The Frontiers Collection. Springer Berlin Heidelberg, 2009.

NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security. Edited by Gary Stoneburner. Gaithersburg, Maryland: National Institute of Standards & Technology, 2001.

NIST Special Publication 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Joint Task Force Transformation Initiative. Gaithersburg, Maryland: National Institute of Standards & Technology, 2010.

NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Joint Task Force Transformation Initiative. Gaithersburg, Maryland: National Institute of Standards & Technology, 2013.

NIST Special Publication 800-70, Revision 2: National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. Edited by Stephen D. Quinn, Murugiah P. Souppaya, Melanie Cook, and Karen A. Scarfone. Gaithersburg, Maryland: National Institute of Standards & Technology, 2011.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers. Edited by P. Bowen, J. Hash, and M. Wilson. Gaithersburg, Maryland: National Institute of Standards & Technology, 2006.

Overman, Stephenie. "Jamming Employee Phones Illegal." Society for Human Resource Management, May 9, 2014. http://www.shrm.org/hrdisciplines/technology/articles/pages/cell-phone-jamming.aspx. Accessed July 22, 2015.

Pająk, Robert. Email correspondence with the author, May 3, 2015.

Panoulas, Konstantinos J., Leontios J. Hadjileontiadis, and Stavros M. Panas. "Brain-Computer Interface (BCI): Types, Processing Perspectives and Applications." In *Multimedia Services in Intelligent Environments*, edited by George A. Tsihrintzis and Lakhmi C. Jain, 299-321. Smart Innovation, Systems and Technologies 3. Springer Berlin Heidelberg, 2010.

Park, M.C., M.A. Goldman, T.W. Belknap, and G.M. Friehs, "The Future of Neural Interface Technology." In *Textbook of Stereotactic and Functional Neurosurgery*, edited by A.M. Lozano, P.L. Gildenberg, and R.R. Tasker, 3185-3200. Heidelberg/Berlin: Springer, 2009.

Parker, Donn "Our Excessively Simplistic Information Security Model and How to Fix It." *ISSA Journal* (July 2010): 12-21.

Parker, Donn B. "Toward a New Framework for Information Security." In *The Computer Security Handbook*, 4th Ed., edited by Seymour Bosworth and M. E. Kabay. John Wiley & Sons, 2002.

Passeraub, Ph A., and N. V. Thakor. "Interfacing Neural Tissue with Microsystems." In *Neural Engineering*, edited by Bin He, 49-83. Bioelectric Engineering. Springer US, 2005.

Patil, P.G., and D.A. Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices." In *Neurotherapeutics* 5, no. 1 (January 1, 2008): 137-46.

Pearce, David, "The Biointelligence Explosion." In *Singularity Hypotheses*, edited by A.H. Eden, J.H. Moor, J.H. Søraker, and E. Steinhart, 199-238. The Frontiers Collection. Berlin/Heidelberg: Springer, 2012.

Polikov, Vadim S., Patrick A. Tresco, and William M. Reichert. "Response of brain tissue to chronically implanted neural electrodes." *Journal of Neuroscience Methods* 148, no. 1 (2005): 1-18.

Prestes, E., J.L. Carbonera, S. Rama Fiorini, V.A.M. Jorge, M. Abel, R. Madhavan, A. Locoro, et al., "Towards a Core Ontology for Robotics and Automation." *Robotics and Autonomous Systems*, Ubiquitous Robotics 61, no. 11 (November 2013): 1193-1204.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Pribram, K. H. "Prolegomenon for a Holonomic Brain Theory." In *Synergetics of Cognition*, edited by Hermann Haken and Michael Stadler, 150-84. Springer Series in Synergetics 45. Springer Berlin Heidelberg, 1990.

Pribram, K.H., and S.D. Meade. "Conscious Awareness: Processing in the Synaptodendritic Web - The Correlation of Neuron Density with Brain Size." *New Ideas in Psychology* 17, no. 3 (December 1, 1999): 205–14. doi:10.1016/S0732-118X(99)00024-0.

Principe, José C., and Dennis J. McFarland. "BMI/BCI Modeling and Signal Processing." In *Brain-Computer Interfaces*, 47-64. Springer Netherlands, 2008.

Proudfoot, Diane. "Software Immortals: Science or Faith?" In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 367-92. The Frontiers Collection. Springer Berlin Heidelberg, 2012.

Qureshi, Mohmad Kashif. "Liveness detection of biometric traits." *International Journal of Information Technology and Knowledge Management* 4 (2011): 293-95.

Rahimi, Ali, Ben Recht, Jason Taylor, and Noah Vawter. "On the effectiveness of aluminium foil helmets: An empirical study." MIT, February 17, 2005. http://web.archive.org/web/20100708230258/http://people.csail.mit.edu/rahimi/helmet/. Accessed July 26, 2015.

Ramirez, S., X. Liu, P.-A. Lin, J. Suh, M. Pignatelli, R.L. Redondo, T.J. Ryan, and S. Tonegawa. "Creating a False Memory in the Hippocampus." *Science* 341, no. 6144 (2013): 387-91.

Rao, R.P.N., A. Stocco, M. Bryan, D. Sarma, T.M. Youngquist, J. Wu, and C.S. Prat. "A direct brain-to-brain interface in humans." *PLoS ONE* 9, no. 11 (2014).

Rao, Umesh Hodeghatta, and Umesha Nayak. *The InfoSec Handbook*. New York: Apress, 2014.

Rasmussen, Kasper Bonne, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. "Proximity-based access control for implantable medical devices." In *Proceedings of the 16th ACM conference on Computer and communications security*, 410-19. ACM, 2009.

Reynolds, Dwight W., Christina M. Murray, and Robin E. Germany. "Device Therapy for Remote Patient Management." In *Electrical Diseases of the Heart*, edited by Ihor Gussak, Charles Antzelevitch, Arthur A. M. Wilde, Paul A. Friedman, Michael J. Ackerman, and Win-Kuang Shen, 809-25. Springer London, 2008.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Robinett, W. "The consequences of fully understanding the brain." In Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science, edited by M.C. Roco and W.S. Bainbridge, 166-70. National Science Foundation, 2002.

Roosendaal, Arnold. "Carrying Implants and Carrying Risks; Human ICT Implants and Liability." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 69-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Roosendaal, Arnold. "Implants and Human Rights, in Particular Bodily Integrity." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 81-96. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rossebeø, J. E. Y., M. S. Lund, K. E. Husa, and A. Refsdal, "A conceptual model for service availability." In *Quality of Protection*, 107-18. Advances in Information Security 23. Springer US, 2006.

Rotter, Pawel, Barbara Daskala, and Ramon Compañó. "Passive Human ICT Implants: Risks and Possible Solutions." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 55-62. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rotter, Pawel, Barbara Daskala, Ramon Compañó, Bernhard Anrig, and Claude Fuhrer. "Potential Application Areas for RFID Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 29-39. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rotter, Pawel, and Mark N. Gasson. "Implantable Medical Devices: Privacy and Security Concerns." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 63-66. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rubin, Charles T. "What Is the Good of Transhumanism?" In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 137-56. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Rutten, W. L. C., T. G. Ruardij, E. Marani, and B. H. Roelofsen. "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe." In *Operative Neuromodulation*, edited by Damianos E. Sakas and

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Brian A. Simpson, 547-54. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Sakas, Damianos E., I. G. Panourias, and B. A. Simpson. "An Introduction to Neural Networks Surgery, a Field of Neuromodulation Which Is Based on Advances in Neural Networks Science and Digitised Brain Imaging." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 3-13. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Sasse, Martina Angela, Sacha Brostoff, and Dirk Weirich. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." *BT technology journal* 19, no. 3 (2001): 122-131.

Sayrafian-Pour, K., W.-B. Yang, J. Hagedorn, J. Terrill, K. Yekeh Yazdandoost, and K. Hamaguchi. "Channel Models for Medical Implant Communication." *International Journal of Wireless Information Networks* 17, no. 3-4 (December 9, 2010): 105-12.

Schechter, Stuart. "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices." Microsoft Research, August 10, 2010. http://research.microsoft.com:8082/apps/pubs/default.aspx?id=135291. Accessed July 26, 2015.

Schermer, Maartje. "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction." *NanoEthics* 3, no. 3 (December 1, 2009): 217-30. doi:10.1007/s11569-009-0076-9.

Shih, J. "Project time in Silicon Valley." *Qualitative Sociology* 27, no. 2 (June 1, 2004): 223-45.

Shoniregun, Charles A., Kudakwashe Dube, and Fredrick Mtenzi. "Introduction to E-Healthcare Information Security." In *Electronic Healthcare Information Security*, 1-27. Advances in Information Security 53. Springer US, 2010.

Smolensky, Paul. "The Constituent Structure of Connectionist Mental States: A Reply to Fodor and Pylyshyn." In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 281-308. Studies in Cognitive Systems 9. Springer Netherlands, 1991.

Soussou, Walid V., and Theodore W. Berger. "Cognitive and Emotional Neuroprostheses." In *Brain-Computer Interfaces*, 109-23. Springer Netherlands, 2008.

Spohrer, Jim, "NBICS (Nano-Bio-Info-Cogno-Socio) Convergence to Improve Human Performance: Opportunities and Challenges." In Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science, edited by M.C. Roco and W.S. Bainbridge, 101-17. Arlington, Virginia: National Science Foundation, 2002.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Srinivasan, G. R. "Modeling the cosmic-ray-induced soft-error rate in integrated circuits: an overview." *IBM Journal of Research and Development* 40, no. 1 (1996): 77-89.

Stahl, B. C. "Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency." *Ethics and Information Technology* 8, no. 4 (2006): 205-13.

Stieglitz, Thomas. "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 435-42. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Szczepocka, Magdalena. "Konflikt sprzecznych utopii jako główny problem gry fabularnej 'Mag: Wstąpienie'." Głos Pana: Utopie i dystopie w kulturze audiowizualnej. Facta Ficta, Jagiellonian University, Kraków, March 27, 2015.

Tadeusiewicz, Ryszard, Pawel Rotter, and Mark N. Gasson. "Restoring Function: Application Exemplars of Medical ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 41-51. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Taira, Takaomi, and T. Hori. "Diaphragm Pacing with a Spinal Cord Stimulator: Current State and Future Directions." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 289-92. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Tamburrini, Guglielmo. "Brain to Computer Communication: Ethical Perspectives on Interaction Models." *Neuroethics* 2, no. 3 (March 11, 2009): 137-49. doi:10.1007/s12152-009-9040-1.

Tarín, C., L. Traver, P. Martí, and N. Cardona. "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring." In *Wireless Technology*, edited by S. Powell and J.P. Shim, 177-201. Lecture Notes in Electrical Engineering 44. Springer US, 2009.

Taylor, N. R., and J. G. Taylor. "The Neural Networks for Language in the Brain: Creating LAD." In *Computational Models for Neuroscience*, edited by Robert Hecht-Nielsen and Thomas McKenna, 245-65. Springer London, 2003.

Taylor, Dawn M. "Functional Electrical Stimulation and Rehabilitation Applications of BCIs." In *Brain-Computer Interfaces*, 81-94. Springer Netherlands, 2008.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Thanos, Solon, P. Heiduschka, and T. Stupp. "Implantable Visual Prostheses." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 465-72. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Thonnard, Olivier, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, and Martin Lee. "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat." In *Research in Attacks, Intrusions, and Defenses*, edited by Davide Balzarotti, Salvatore J. Stolfo, and Marco Cova, 64-85. Lecture Notes in Computer Science 7462. Springer Berlin Heidelberg, 2012.

Thorpe, Julie, Paul C. van Oorschot, and Anil Somayaji. "Pass-thoughts: authenticating with our minds." In *Proceedings of the 2005 Workshop on New Security Paradigms*, 45-56. ACM, 2005.

Troyk, Philip R., and Stuart F. Cogan. "Sensory Neural Prostheses." In *Neural Engineering*, edited by Bin He, 1-48. Bioelectric Engineering. Springer US, 2005.

Ullah, Sana, Henry Higgin, M. Arif Siddiqui, and Kyung Sup Kwak. "A Study of Implanted and Wearable Body Sensor Networks." In *Agent and Multi-Agent Systems: Technologies and Applications*, edited by Ngoc Thanh Nguyen, Geun Sik Jo, Robert J. Howlett, and Lakhmi C. Jain, 464-73. Lecture Notes in Computer Science 4953. Springer Berlin Heidelberg, 2008.

U.S. Code, Title 44 (Public Printing and Documents), Subchapter III (Information Security), Section 3542 (Definitions), cited in *NIST Special Publication 800-37, Revision 1.*

Vildjiounaite, Elena, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices." In *Pervasive Computing*, edited by Kenneth P. Fishkin, Bernt Schiele, Paddy Nixon, and Aaron Quigley, 187-201. Lecture Notes in Computer Science 3968. Springer Berlin Heidelberg, 2006.

Viola, M. V., and Aristides A. Patrinos. "A Neuroprosthesis for Restoring Sight." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 481-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Warwick, K. "The cyborg revolution." *Nanoethics* 8 (2014): 263-73.

Warwick, K., and M. Gasson, "Implantable Computing." In *Digital Human Modeling*, edited by Y. Cai, 1-16. Lecture Notes in Computer Science 4650. Berlin/Heidelberg: Springer, 2008.

Weber, R. H., and Weber, R. "General Approaches for a Legal Framework." In *Internet of Things*, 23-40. Springer Berlin/Heidelberg, 2010.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Weiland, James D., Wentai Liu, and Mark S. Humayun. "Retinal Prosthesis." *Annual Review of Biomedical Engineering* 7, no. 1 (2005): 361-401. doi:10.1146/annurev.bioeng.7.060804.100435.

Weinberger, Sharon. "Mind Games." The Washington Post, January 14, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399_pf.html. Accessed July 26, 2015.

Werkhoven, Peter. "Experience Machines: Capturing and Retrieving Personal Content." In *E-Content*, edited by Peter A. Bruck, Zeger Karssen, Andrea Buchholz, and Ansgar Zerfass, 183-202. Springer Berlin Heidelberg, 2005.

Widge, A.S., C.T. Moritz, and Y. Matsuoka. "Direct Neural Control of Anatomically Correct Robotic Hands." In *Brain-Computer Interfaces*, edited by D.S. Tan and A. Nijholt, 105-19. Human-Computer Interaction Series. London: Springer, 2010.

Wiener, Norbert. *Cybernetics: Or Control and Communication in the Animal and the Machine*, second edition. Cambridge, Massachusetts: The MIT Press, 1961 (Quid Pro ebook edition for Kindle, 2015).

Wilkinson, Jeff, and Scott Hareland. "A cautionary tale of soft errors induced by SRAM packaging materials." *IEEE Transactions on Device and Materials Reliability* 5, no. 3 (2005): 428-433.

Wiltshire, Travis J., Dustin C. Smith, and Joseph R. Keebler. "Cybernetic Teams: Towards the Implementation of Team Heuristics in HRI." In *Virtual Augmented and Mixed Reality. Designing and Developing Augmented and Virtual Environments*, edited by Randall Shumaker, 321-30. Lecture Notes in Computer Science 8021. Springer Berlin Heidelberg, 2013.

Zamanian, Ali, and Cy Hardiman. "Electromagnetic radiation and human health: A review of sources and effects." *High Frequency Electronics* 4, no. 3 (2005): 16-26.

Zarod, Marcin. "Constructing Hackers. Professional Biographies of Polish Hackers." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Zebda, Abdelkader, S. Cosnier, J.-P. Alcaraz, M. Holzinger, A. Le Goff, C. Gondran, F. Boucher, F. Giroud, K. Gorgy, H. Lamraoui, and P. Cinquin. "Single glucose biofuel cells implanted in rats power electronic devices." *Scientific Reports* 3, article 1516 (2013). doi:10.1038/srep01516.

Zhao, QiBin, LiQing Zhang, and Andrzej Cichocki. "EEG-Based Asynchronous BCI Control of a Car in 3D Virtual Reality Environments." *Chinese Science Bulletin* 54, no. 1 (January 11, 2009): 78-87. doi:10.1007/s11434-008-0547-3.

Chapter 5, "A Two-dimensional Framework of Cognitional Security for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 129-168.

Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, and Rajan Shankaran. "A Non-key based security scheme supporting emergency treatment of wireless implants." In *2014 IEEE International Conference on Communications (ICC)*, 647-52. IEEE, 2014.

Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, Rajan Shankaran, and Eryk Dutkiewicz. "Securing wireless medical implants using an ECG-based secret data sharing scheme." In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, 373-77. IEEE, 2014.

Zheng, Guanglou, Gengfa Fang, Rajan Shankaran, Mehmet Orgun, and Eryk Dutkiewicz. "An ECG-based secret data sharing scheme supporting emergency treatment of Implantable Medical Devices." In *2014 International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 624-28. IEEE, 2014.