*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Chapter Three

Critical Challenges in Information Security for Advanced Neuroprosthetics

Information security considerations unique to advanced neuroprosthetics

Information security is a large and complex field. While there are fundamental information security principles whose relevance is universal, the ways in which these principles are applied and elaborated in particular circumstances is subject to specialized practices and bodies of knowledge. The techniques used to secure a large organization's archive of decades of printed personnel files are different than those used to secure a factory's robotic manufacturing systems or an individual consumer's smartphone.

As with all kinds of information systems that have been developed by humankind, advanced neuroprosthetic devices present a unique array of information security problems and possibilities that exist within a particular set of technological, legal, political, ethical, social, and cultural contexts.[1] In this chapter we highlight a number of issues that may not be relevant for many other kinds of information systems but which give rise to considerations that are critical for the information security of advanced neuroprosthetic devices. Many of the issues discussed below constitute recurring themes that will be revisited in different contexts throughout the rest of this book.

Device user vs. device host

In the case of a smartphone, the person who possesses the device and carries it with himself or herself on a daily basis is typically also the primary user and operator of the device: the smartphone's possessor powers it on and off,

[1] For an overview of ethical issues with ICT implants – many of which are relevant for advanced neuroprosthetics – see Hildebrandt & Anrig, "Ethical Implications of ICT Implants" (2012). For ethical issues in information security more generally, see Brey, "Ethical Aspects of Information Security and Privacy" (2007).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

uses it to browse the web, check email, make calls, and play games, and downloads, installs, and uninstalls apps at will. In some institutional settings, a smartphone that is owned by the organization may not be controlled entirely by the person who possesses it; the organization's IT staff might remotely control and monitor some aspects of the phone's behavior and might, for example, restrict its possessor's ability to install new apps. However, the person possessing the phone still has a significant ability to control the device's settings and operation and to use its functionality to achieve his or her personal ends.

With advanced neuroprosthetic devices (and implantable medical devices generally) the situation can be quite different: a device's host – i.e., the human being in whose body the neuroprosthetic device is implanted and in which it operates – may have no ability whatsoever to control the device or to utilize its functionality for particular ends chosen by that person. Moreover, he or she may not even realize that the device exists and has been integrated into his or her neural circuitry.

Shared operation and use by the host and an external party

In the case of an artificial eye, for example, it might be the case that the device's human host has full operational control over the device: through an act of volition, the host transmits instructions that cause the eye to focus its gaze on particular objects, and by using a standard computer the host can wirelessly connect to the artificial eye's internal computer, log onto a web-based command console, and perform remote diagnostics and software maintenance on the device.

On the other hand, it might be the case that the device's human host is only able to control some limited aspects of the artificial eye's functionality (such as determining its focus or dilating its synthetic pupil) but has no ability to log into the device to manage diagnostic or maintenance tasks; a remote support team of specialized medical and biomedical engineering experts (e.g., working at the company that designed the device or the hospital that implanted it) may be the only party with such access – regularly monitoring the device's functioning, performing remote software upgrades and reconfiguration, and managing aspects such as the device's power consumption and synaptic stimulation strength. In such a scenario, the human being in whom the artificial eye was implanted would be the device's human *host*, but the host and the remote medical team would share a joint role as the device's *users* or *operators* who determine how and for what purposes it will be used and who control its functionality.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Separate operator and host

It is also possible to envision circumstances in which a device's human host would play no role at all in controlling the device, determining the purposes for which it will (or will not) be employed, or managing its functionality. In such cases, another human being or organization may serve as the sole user and operator of the device, or, if the device possesses sufficiently sophisticated artificial intelligence, the device could even be said to be its own user and operator.

For example, a human host suffering from a particular illness may have been implanted with an endocrine neuroprosthetic device that can stimulate the host's thyroid gland and cause it to secrete hormones that affect the body's basal metabolic rate; however, the host has no means or access by which to control (or even directly influence) the functioning of the device, as it can only be controlled through a remote system that wirelessly transmits instructions to the device and is managed by an expert medical team. The medical team constitutes the device's sole user and operator, as team members decide when, whether, and to what extent the host's basal metabolic rate should be raised or lowered, and the medical personnel determine the objective (e.g., to facilitate weight loss or weight gain) that they are seeking to achieve through their management of the device.[2]

Unwitting hosts

Especially in the case of noninvasive neuroprosthetic devices that can connect with the neural circuitry of a human being simply by touching the person's body (or even without touching it, through the use of wireless transmission and sensation), it may be possible that the human being with whose neurons the device is interacting may not even realize that the device exists or is in use. Even in the case of neuroprosthetic devices that can only function within the body of their human host, a device's host may potentially not realize that a neuroprosthetic device is located and operating within his or her body – e.g., if unbeknownst to the subject the device was implanted during the course of some other surgical procedure to which the host had consented, or if the device comprised components (such as a swarm of nanorobots) that could be unwittingly ingested by consuming a beverage.[3]

---

[2] Another possible cybernetic model is for a system to include an implanted component that gathers from its host's brain selected real-time data that is then transmitted to an external system and used as input for a real-time computational model and simulation of the brain that allows the device's operators to determine what signals the implanted component should transmit to neurons in order to generate desired effects; the external system then transmits those instructions to the implanted component, which then stimulates neurons in accordance with those instructions. See Lee et al., "Towards Real-Time Communication between in Vivo Neurophysiological Data Sources and Simulator-Based Brain Biomimetic Models" (2014).

[3] For the possibility that human hosts might unwittingly have been implanted with RFID devices,

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Physical and psychological damage caused to user or host

In numerous contexts throughout this text, we cite the possibility that a neuroprosthetic device that is poorly designed and operated, suffers a malfunction, or is compromised by a cyberattack could potentially subject its human host to significant physical or psychological harm – e.g., by impairing the functioning of the host's internal organs or providing a stream of sensory data that causes severe pain. While such harm to a device's host may be the more common hazard, with some kinds of neuroprosthetic devices it possible that such incidents might cause physical or psychological harm to the device's human *operator* rather than its *host*.

For example, imagine that a human host has – without his or her knowledge – been implanted with an advanced neuroprosthetic device located in the brain that detects sense data arriving from the optic and cochlear nerves and wirelessly transmits it to another human being – the device's operator – who through the use of a virtual reality headset and earphones is essentially able to see and hear all that the neuroprosthetic device's human host sees and hears. An adversary could potentially gain unauthorized access to the neuroprosthetic device's internal computer, reprogram it, disable its safety features, and alter its output so that rather than transmitting to the device's remote human operator a stream of the actual visual and auditory sense data received by the device's host it instead transmitted signals which, in the operator's VR headset and earphones, produce an emission of blinding light and deafening noise that are powerful enough to both damage the operator's sensory organs, cause confusion and disorientation, and inflict major psychological distress. Note that if the operator (and, in this case, end user) of the neuroprosthetic device were receiving the transmitted sense data not through a conventional VR headset and set of earphones but through a neuroprosthetic implant within his or her own brain, then an arrangement would exist in which that individual was simultaneously serving as the host of one neuroprosthetic device and the operator of (potentially) two devices, and the damage would result from the person's roles both as host of his or her own implanted device and operator of the remotely controlled one.

Critical, noncritical, or no health impacts for a device's host and user

A conventional desktop computer is unlikely to have a direct critical impact (either positive or negative) on the health of its human user. While it is

---

see Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

possible to imagine a critical health impact (e.g., if the computer electrocuted a user who had removed the outer casing and was attempting to repair the device or if the user dropped the computer and injured himself or herself while attempting to carry it to a new location), such impacts involve highly unusual circumstances and do not result directly from the success or failure of the computer to perform its intended regular functions. It is perhaps more likely for a computer to have an impact on its user's health that is critical but highly indirect – e.g., by allowing its user to contact emergency medical personnel and summon assistance with some urgent health emergency or to research symptoms that the user was experiencing and diagnose a major illness.

Because of their intimate integration into the body and biological processes of their human host, however, neuroprosthetic devices have the potential to directly generate critical health impacts for human beings that other kinds of information systems are unlikely or unable to produce.[4] For example, the failure of a neuroprosthetic device that is responsible for regulating its host's respiratory or circulatory activity could result directly in the host's death within a matter of minutes or even seconds; conversely, the proper functioning of the device may extend its host's lifespan by many years. Such devices clearly possess a critical health impact.

Other kinds of technology, such as a neuroprosthetic robotic leg, may typically have a significant but indirect and noncritical impact on the health of its user. When functioning properly, the leg allows its user to stand and balance without falling and to walk, run, and exercise – all of which can contribute significantly (if not critically) to the user's health. On the other hand, if the device experiences a malfunction that gives the user mild electrical shocks or requires the user to drag the immobile leg, such occurrences would constitute undeniably negative but generally noncritical health effects. Such device malfunctions call for prompt attention and maintenance but do not require an immediate response in order to save the life of the device's host.

Even with devices that generally demonstrate noncritical health impacts, it may be possible for them to yield a critical health impact in particular circumstances. For example, if an artificial eye were to fail while its host were driving an automobile or flying a helicopter, this could potentially have fatal consequences not only for the host but also for many other completely unrelated individuals. A similarly critical negative health impact could result if an adversary gained unauthorized access to the eye's internal computer and manipulated the device's sensory output to make its host believe, for example,

[4] For some of the health impacts that can be generated, for example, by IMDs (whether neuroprosthetic devices or other kinds of IMDs), see Ankarali et al., "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security" (2014).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

that he or she was picking up a wooden stick from the lawn when in fact it was a poisonous snake.[5]

No matter how safe, limited, and benign its functionality might be, it is unlikely that any neuroprosthetic device could ever possess *no* health impact, insofar as it is by definition interacting with the neural circuitry of its human host. While some advanced devices might theoretically be able, for example, to remotely detect and interpret a human being's cognitive activity simply by relying on the passive capture of radiation or other phenomena naturally emitted by the person's brain – and thus allow the person to control some remote robotic system through thought alone – such a device would not be considered a "neuroprosthetic device" according to the definition of this text, since it is not truly *integrated into* the neural circuitry of the person's brain or body in any substantive sense.

Note that when a neuroprosthetic device possesses (or has the potential to demonstrate) a critical health impact, ensuring information security for the device and its host and user becomes even more important than usual. The greatest possible attention to information security must be shown by such a device's designer, manufacturer, operator, and host; such a device is likely to need extremely robust and stringent security controls that may not be necessary for devices with a lesser potential health impact. This obligation to ensure the highest possible degree of information security for neuroprosthetic devices with a (potentially) critical health impact will inform our discussions of many specific security practices and mechanisms throughout this text.

Lack of direct physical access to implanted systems

Because of the risks and difficulties involved with surgical procedures, after a neuroprosthetic device has been implanted in its human host, information security personnel working to protect that device and its host may never again enjoy the opportunity to physical inspect, manipulate, or otherwise access the device; from that point forward, the only means of interacting with the device may be through wireless communication[6] (assuming that the device possesses such capabilities) or through action of the device's host (e.g.,

[5] For the possibility that sensory neuroprosthetics might be used to supply false data or information to their hosts or users, see McGee, "Bioelectronics and Implanted Devices" (2008), p. 221.

[6] For an overview of information security issues relating to the wireless communication of IMDs such as body sensor networks (BSNs) – many of which are relevant for advanced neuroprosthetics – see Ameen et al., "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

if the host has the ability to communicate with, influence, or control the device through acts of volition or other internal cognitive or biological processes). On the one hand, such limitations in physical access may create challenges for information security personnel: for example, it may be necessary to build into a device at the time of its creation and implantation security controls that will be powerful and adaptable enough to counteract threats that may not yet even exist and will be developed only years or decades after the device's implantation. Moreover, some physical security controls that can be applied to conventional computers (such as the use of hardwired rather than wireless communication between devices) may be impossible to apply to an implanted device that exists beyond one's grasp and direct physical control. On the other hand, the fact that a neuroprosthetic device has been implanted in a human host might also bring some security benefits (such as physical concealment of the device's existence[7]) that are more difficult to implement in other kinds of information systems such as desktop computers.

100% availability required

From the perspective of information security, the information contained within particular information systems can be said to demonstrate "availability" if the "systems work promptly and service is not denied to authorized users;"[8] other information security experts have defined availability as "Ensuring timely and reliable access to and use of information"[9] or the "Usability of information for a purpose."[10] These are the meanings of availability that are intended, for example, when the word is used as part of the CIA Triad of information security objectives.

Other branches of computer science and information technology, however, use the word "availability" with an equally specific but somewhat different meaning: in that alternative sense, an information system's availability is a quantitative measure of how likely it is that the system will be operational (i.e., not out of service due to some hardware or software fault) at a given point in time. One can quantify a computer's **reliability** as the **mean time to failure** (MTTF), or the average length of time that a system will remain in continuous operation before experiencing its next failure,[11] while the **mean**

---

[7] Regarding the use of physical concealment in protection information systems, see *NIST SP 800-53*, Rev. 4 (2013), p. F-205-F-206.

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

[9] 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37*, Rev. 1 (2010), p. B-2.

[10] See Parker, "Toward a New Framework for Information Security" 2002, p. 124.

[11] See Grottke et al., "Ten fallacies of availability and reliability analysis" (2008), as cited in Gladden, "A Fractal Measure for Comparing the Work Effort of Human and Artificial Agents Performing Management Functions" (2014), from which this section on availability is adapted.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

time to repair (MTTR) is the average length of time needed to detect and repair a failure after it has occurred and thereby return the system to operation. A computer's steady-state **availability** *A* can be defined as the likelihood that the system is operating at a particular moment; it is related to the system's MTTF and MTTR by the equation:[12]

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

A typical requirement for general-purpose commercial computer systems is that they demonstrate 99.99% availability over the course of a year.[13] However, in the case of some neuroprosthetic devices that level of availability could be wholly unacceptable, insofar as it would represent an average of roughly 53 minutes of downtime over the course of a year. With some kinds of advanced neuroprosthetic devices that regulate critical circulatory or respiratory functions within their host's body, the impact of a device ceasing to operate for a period of 53 consecutive minutes could prove fatal to its human host. On the other hand, for other kinds of devices a period of 53 consecutive minutes in which the device was nonfunctional might not be particularly harmful – especially if the outage took place as part of a scheduled repair process and a medical support team was ready to monitor and treat the device's host during that period, or if the host possessed a reliable backup system that he or she could easily activate during the one hour a year when the primary device typically became nonfunctional.

For some kinds of neuroprosthetic devices, a single long outage once per year might be less harmful than many frequent outages of shorter duration. For example, a system that freezes up and becomes nonfunctional for one millisecond out of every 10 seconds would also demonstrate roughly 99.99% availability. If such a neuroprosthetic device serves as the controller of a complex device network in which it receives data from and coordinates the actions of a number of other implanted devices regulating its host's core biological functions, such frequent outages could potentially impair the work of the entire system – especially if the system needs a couple of seconds to confirm the system's integrity and regain full operational capacity after each millisecond outage.

---

[12] See Grottke et al., "Ten fallacies of availability and reliability analysis" (2008).

[13] See Gunther, "Time—the zeroth performance metric" (2005).

Chapter 3, "Critical Challenges in Information 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. 59-103.

The question of how much time is needed to *fully recover* complete operational capacity by a system whose outage has already ended and which is already nominally functional raises another question relating to availability. In the sense just described here, availability has traditionally been understood in a binary manner: a system is either "up" or "down," with no possible states in between.

While the binary definition of availability is conceptually elegant and results in an equation that is easy to apply, the binary definition completely fails to capture many of the difficult realities with which IT professionals must often grapple. For example, if a hardware failure, software configuration error, or denial of service attack dramatically impacts an organization's information system and reduces the system's performance to only 0.5% of its normal processing speed and capacity, the lived experience of many people in the organization may be that the system is experiencing a catastrophic outage and is wholly nonfunctional. However, according to the technical definition of availability just given, one would say that the system has not "failed," because the system has not failed *completely*; although the system's performance has been dramatically degraded, the system is still operational and functional – simply at a reduced level of speed and capacity. In order to address such limitations with the binary definition of availability, Rossebeø et al. argue that a more sophisticated measure for availability is needed that takes into account qualitative aspects of a system's performance and which recognizes a range of intermediate qualitative states between simply "up" and "down."[14] This is especially true for many kinds of advanced neuroprosthetic devices.

For example, imagine that a high-resolution artificial eye provides its host with output sense data corresponding to a field of vision consisting of five million pixels; that is arguably roughly comparable to the resolution offered by a natural human eye.[15] When operating at such a level, one could say that the system is fully operational and that both the information system (constituted by the artificial eye) and the system's information (constituted by raw sense data from the external environment that has been processed by the device and outputted to its human host) are available. However, during moments of especially high demand on the device's internal processor (e.g., when it is performing a major diagnostic operation or undergoing a software

[14] See Rossebeø et al., "A conceptual model for service availability" (2006).

[15] The question of the human eye's "resolution" is quite complicated. While an eye contains many more than one million sensors (i.e., individual rods and cones), there are only about one million output neurons (in the form of ganglion cells) that transmit data from the eye to the brain, and roughly half of the data comes from the tiny fovea, or focal point at the center of the field of vision in which the eye provides sharp central vision. See Linsenmeier, "Retinal Bioengineering" (2005), for a discussion of some such issues.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

upgrade) the field of vision provided by the device's output data degrade to perhaps, say, only 5,000 total pixels. Although this would represent a dramatic 99.9% reduction in performance (as measured by resolution), it would still be sufficient to allow its host to carry out such tasks as navigating around a room, recognizing faces, or reading text on a computer screen.[16] If one were restricted to a binary definition of availability, one would need to say that the information system and its information were both "available," because the system was indeed functioning and making information available, if to a limited degree.

Imagine further that a major sensor component within the artificial eye fails and the device switches instantaneously to a rudimentary backup sensory of quite limited capacity: as a result, the output data produced by the device represents a visual field of only 64 total pixels. Such limited visual data would likely be insufficient to give the device's host the ability to perform even basic tasks such as navigating visually around a room or recognizing a particular face. In this situation, a binary measure of availability would tell us that the information system and information are still available: the device, after all, is functioning and providing its human host a constant stream of data that represents (in a very limited fashion) the raw sense data received from the external environment. However, from the perspective of information security it would be difficult to say without qualification that the information system and its information were "available" in the sense envisioned by the CIA Triad. If an adversary had launched a cyberattack and gained unauthorized access to the artificial eye in an effort to steal visual information that reveals where the device's host is and what he or she is doing, the adversary would likely not feel satisfied with gaining access to a display of 64 pixels that contains no practically interpretable, *useful* information about the host's external environment or the host's activities.

When considering "availability" in its sense of the functionality or operationality of an information system, one must thus carefully consider whether the measure should be defined in a binary manner in which "availability" signifies any non-zero level of functionality; whether the measure should be defined in a binary manner in which "availability" signifies a level of functionality greater than some particular specified non-zero threshold; or whether a non-binary, multivalent understanding of availability is more appropriate.

For certain kinds of neuroprosthetic devices with critical health impacts, simply setting and meeting a target like 99.99% availability or even 99.999%

[16] See Weiland et al., "Retinal Prosthesis" (2005), and Viola & Patrinos, "A Neuroprosthesis for Restoring Sight" (2007).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

availability (the so-called "five nines" level of availability, equivalent to roughly five minutes of downtime per year) may not be sufficient, as such periods of downtime could be harmful or even fatal to the devices' human host. For some kinds of devices, the only target that is acceptable from a legal and ethical perspective may be that of 100% availability – even if it is known in advance that this may be unattainable, due to circumstances beyond the control of a device's designer, manufacturer, operator, or host. The existence of critical health impacts and the need for 100% availability can be understood in relation to the concept of a zero-day vulnerability in information security, in which software or hardware developers must work as quickly as possible to develop a patch or fix for an uncorrected flaw.

The need for rigorous security vs. the need for instant emergency access

The fact that advanced neuroprosthetic devices are integrated into the neural circuitry of their human host creates a unique information security challenge – and potentially a dilemma – for the developers of such technologies.

The need to protect a device from unauthorized parties

On the one hand, a neuroprosthetic device ought to be better secured against computer viruses and unauthorized access than, say, its host's laptop computer or smartphone. After all, if a person's smartphone is compromised, it could potentially result in inconvenience, financial loss, identity theft, the disclosure of sensitive and embarrassing information, and potentially even legal liability for that person – but it is unlikely to have a direct critical impact on the person's physical health. If a person's neuroprosthetic device is compromised, though, this might not only allow an adversary to steal sensitive medical data and information about the person's cognitive activity (potentially even including the contents of sensory experiences, memories, volitions, fears, or dreams); it might also – through the device's impact on the person's natural neural networks – have the effect of rendering damaged, untrustworthy, or inaccessible the information stored within the host's natural biological systems, including the brain's memory-storage mechanisms.[17] The potential impact of the intentional manipulation or accidental corruption of a neuroprosthetic device could be potentially catastrophic for the physical and psychological health of its human host; this suggests that access to such a device should be limited to the smallest possible number of human agents

[17] For the possibility that an adversary might use a compromised neuroprosthetic device in order to alter, disrupt, or manipulate the memories of its host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

who are critical to its successful functioning, such as the device's human host and – if a different person – its primary human operator.

The need to grant emergency device access to outside parties

On the other hand, though, there are reasons why restricting access to a neuroprosthetic device too severely might also result in significant harm to the device's host. For example, imagine that the human host of a neuroprosthetic device has been involved in a serious accident or is unexpectedly experiencing an acute and life-threatening medical incident. In this case, emergency medical personnel on the scene may need to gain immediate access to the neuroprosthetic device and exercise unfettered control over its functionality in order to save the life of its host.[18] The same mechanisms that make it difficult for a cybercriminal to break into the neuroprosthetic device – such as proprietary security software, file encryption, and a lack of physically accessible I/O ports – would also make it difficult or impossible for emergency medical personnel to break into the device. In principle, government regulators could require (or the manufacturers of neuroprosthetic devices could voluntarily institute) mechanisms that allow such devices to be accessed by individuals presenting certain credentials that identify them as certified emergency medical personnel who are trained in the use of such technologies,[19] or neuroprosthetic devices could be designed to temporarily disable some of their security controls if they detect that their host is experiencing a medical emergency.[20] However, such mechanisms themselves create security vulnerabilities that could potentially be exploited by an adversary who is highly motivated to gain access to the information contained in a neuroprosthetic device or its human host.

Proposed methods for balancing these competing demands

Ideally, a neuroprosthetic device (and especially one with a critical health impact for its host) would be utterly impervious to all attacks and impenetrable to any adversaries attempting to gain unauthorized access – but would

---

[18] See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012); Rotter & Gasson, "Implantable Medical Devices: Privacy and Security Concerns" (2012); and Halperin et al., "Security and privacy for implantable medical devices" (2008) – all of whom who make this point regarding IMDs. Halperin et al., especially, consider this question in detail.

[19] For a discussion of such certificate schemes and related topics, see, for example, Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), and Freudenthal et al., "Practical techniques for limiting disclosure of RF-equipped medical devices" (2007).

[20] Regarding the ability of IMDs to detect a medical emergency that is being experienced by their human host, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), pp. 921-22.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

instantaneously grant full access and place itself at the disposal of any trained and well-intentioned individual who, in time of need, was attempting to use the device to save its human host's life. In reality, it is difficult to design a device that simultaneously fulfills both of these visions, and trade-offs often need to be made. The priorities that a particular host adopts for his or her neuroprosthetic device's information security plan may partly depend on what the host considers to be more likely: that that a corporate espionage agent or cybercriminal will someday attempt to break into his or her neuroprosthetic device in order to steal the person's memories or arrange the person's death, or that an emergency medical technician will someday need to break into the device and override its programmed functioning in order to deliver life-saving medical treatment or prevent the host from suffering some grave neurological damage.

Hansen and Hansen note that the controls and countermeasures designed to protect implantable medical devices from unauthorized access while simultaneously ensuring that authorized parties (such as emergency medical personnel) receive access typically take one of three forms, as either **detective**, **protective**, or **corrective** countermeasures. For example, a security control that alerts a device's human host to a series of unsuccessful logon attempts would be detective, one that blocks wireless transmissions from reaching an implanted device would be protective, and one that allows compromised data within the device's internal memory to be replaced by backup data from an external system would be corrective.[21] Below we consider a number of specific controls and countermeasures that have been proposed to address the challenge of providing both rigorous protection for implanted devices and robust emergency access for authorized personnel. While some of these approaches may not be relevant for all kinds of neuroprosthetic devices (especially devices that operate outside of their host's body), many of the approaches are relevant for implantable neuroprosthetic devices, and they offer an excellent starting point for considering issues of emergency access for neuroprosthetic devices more broadly.

Certificate schemes and predeployed keys managed by device manufacturers or operators

One approach to addressing this challenge involves the creation of a centrally managed worldwide certification scheme that would be administered either by a device's manufacturer or operator. At the time of its manufacture or implantation, a pre-configured backdoor key can be installed in the operating system of an IMD; the backdoor key can be maintained by the device's

[21] See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

manufacturer or operator in a cloud-based system that can be accessed globally through the Internet by medical personnel who are treating the device's host during the course of a medical emergency.[22]

However, this model demonstrates significant limitations and disadvantages. Hei and Du note that this "certificate" approach would fail in cases where the medical emergency (and treatment) were occurring in a location in which the personnel providing medical treatment did not have immediate Internet access (e.g., if an accident occurred in a remote wilderness area where wireless Internet access was absent or unreliable); moreover, they note that maintaining such a system of backdoor keys that are always accessible online would be complex and costly.[23]

An external hardware token whose possession grants access to the implanted device

Bergmasco et al. explore the use of hardware tokens such as a small USB token that can be inserted into a standard USB port as means of authenticating users of medical devices and information systems.[24] External hardware tokens that utilize wireless technologies – such as an RFID tag worn or carried by the host of a neuroprosthetic device – could potentially be used by the implanted device to wirelessly authenticate its user; even technologies such as a USB token that require physical insertion of the token into the implanted device could conceivably be used for authentication if the implanted device possesses a port, slot, or other component that is accessible from the exterior of its host's body. Denning et al. describe a similar approach of "proximity bootstrapping" in which emergency medical personnel who may come into contact with patients possessing implantable medical devices could be given a portable unit that can communicate with an IMD through sound waves or "physiological keying" when brought into contact with the device's host to request access to the IMD.[25]

---

[22] For a discussion of such matters, see, for example, Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), and Freudenthal et al., "Practical techniques for limiting disclosure of RF-equipped medical devices" (2007).

[23] See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011).

[24] See Bergamasco et al., "Medical data protection with a new generation of hardware authentication tokens" (2001). They do not specifically consider the case of implantable medical devices but instead consider access to medical devices and information systems more generally.

[25] See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), p. 922.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Hei and Du note that such an external hardware token can be lost (thus denying emergency access to an authorized party who has misplaced his or her token) or stolen (thus potentially granting access to an unauthorized party who has stolen or found the device).[26] We would also note that unless there is international regulation or extensive industry-wide (and even inter-industry) collaboration between the manufacturers of diverse kinds of implantable devices to agree on a single shared scheme for such tokens, the need for emergency personnel around the world to carry a bewildering array of tokens for different manufacturers' devices (and perhaps to test them all on every newly encountered patient in order to check whether any implanted devices might exist) could become unwieldy. On the other hand, if all device manufacturers were to utilize a single shared token system, this would give potential adversaries a lone attractive target on which to concentrate all of their efforts to compromise such devices.

A cryptographic key stored on the host's person

One design for a security control is for wireless access to an implanted device to be secured using a cryptographic key (e.g., consisting of a string of characters) that must be possessed by any other implant or external device that wishes to access the implant. The cryptographic key – along with instructions to emergency medical personnel describing the nature of a host's implanted device and how medical personnel should access and configure the device during particular kinds of medical situations – could then be displayed on a standard medical bracelet worn by the device's host, similar to the sort that is already commonly used by individuals to alert emergency medical personnel to the fact that, for example, they suffer from diabetes or asthma or possess a pacemaker. However, such bracelets are not extremely secure: they can potentially be lost or stolen, may actually alert adversaries to the presence of an implantable device that they otherwise would not have known about, and (depending on their design) could potentially allow an adversary to photograph or otherwise obtain the information contained on the bracelet without even directly contacting it.[27] A card displaying the cryptographic key or password for an implanted device that is carried in the wallet of the device's human host[28] is less visible to potential adversaries while still likely to be found by emergency medical personnel treating the host.

---

[26] See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011).

[27] See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010), and Schechter, "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices" (2010).

[28] See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Denning et al. and Schechter propose an access control method for implantable medical devices that utilizes ultraviolet-ink tattoos.[29] In this approach, an IMD is secured using a cryptographic key consisting of a string of characters. These characters can then be tattooed on the body of the device's host using a special ink that only becomes visible under ultraviolet light. Schechter notes that unlike a wearable accessory such as a bracelet that is used to store the cryptographic key, a tattoo cannot be lost or misplaced by a device's host; moreover, the existence of the tattoo is not readily apparent to potential adversaries, and if necessary the device's host could even prevent a suspected adversary from illuminating and reading the tattoo simply by applying sunscreen that sufficiently blocks ultraviolet light. In comparison to the use of a bracelet, one disadvantage of this approach is the fact that emergency medical personnel would have no immediate indication that the tattoo exists; they would only know to search for a tattoo if they had some particular reason for suspecting that the human subject whom they were treating might possess an implantable device secured by such a cryptographic key. Moreover, emergency medical personnel might not always have the correct sort of UV light available. On the other hand, if the use of UV-ink tattoos for such purposes someday became widespread, then it could conceivably become a standard practice for medical personnel to carry such UV lights and check all patients for the presence of such tattoos. An alternative would be a traditional tattoo that is visible to the naked eye,[30] which would be more likely to be noticed by emergency personnel but would also be more likely to alert an adversary to the existence of an implanted device and allow him or her to obtain the cryptographic key from the tattoo (e.g., since depending on its location on the host's body it could potentially be photographed from a distance).

Denning et al. note that the same sort of severe accident or injury that might require a device's host to receive emergency medical treatment might also damage or destroy the information contained in a tattoo or a medical bracelet worn on the host's person, thus creating a significant disadvantage for such approaches.[31]

---

[29] See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), and Schechter, "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices" (2010).

[30] See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

[31] See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), p. 920.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Access control based on ultrasonic proximity verification

Rasmussen et al. propose a model of access control for implantable medical devices in emergency situations that relies on ultrasound technology to verify the physical proximity of an external system attempting to gain access to the IMD. Under normal circumstances, the IMD would require an external system to possess a shared cryptographic key in order to grant the external system access to the IMD; however if the IMD detects that its host is undergoing a medical emergency, it then shifts into an "emergency mode" in which any external system is allowed to access the IMD, as long as it is within a certain predefined distance – with the distance determined by measuring the time required for ultrasound communications to travel between the IMD and external system.[32]

Hei and Du note that while relying on such ultrasound proximity detection as a primary security control would be inappropriate in normal everyday circumstances (as the control would only function successfully if it could be assumed that the device's host would typically recognize an approaching adversary and prevent him or her from getting to close to the host), it could be appropriate for use in emergency circumstances; they also note that it could be difficult to integrate a sufficiently powerful and effective ultrasound receiver into some kinds of implantable devices.[33]

Physical radio frequency shielding of an implanted device

Hansen and Hansen suggest that a simple means of securing IMDs against wireless RF attacks would be for a device's host to wear a shielded undershirt or shielded bandages applied to the skin that block or disrupt wireless communications. They note that such electromagnetic shielding would be relatively lightweight (thus not greatly inconveniencing the device's host) and could easily be removed by emergency medical personnel who need to treat the host during a critical health situation.[34]

Such an approach is not without disadvantages when applied to advanced neuroprosthetic devices. For many human hosts, being required to wear a special shielded undershirt or bandages wherever they go (e.g., while at the beach or taking a shower) may be an undesirable inconvenience in their daily life, and some hosts might choose to temporarily remove the shielding during such situations, leaving them vulnerable to attack. Moreover, those hosts

---

[32] See Rasmussen et al., "Proximity-based access control for implantable medical devices" (2009). Regarding the possibility of IMDs being able to detect a medical emergency that is being experienced by their human host, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), pp. 921-22.

[33] See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011).

[34] See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

whose neuroprosthetic devices are implanted in their brain would need to wear a shielded hat, wig, bandage, or other appliance on their heads at all times, which can be more awkward and inconvenient than wearing a shielded undershirt and may also serve to draw adversaries' attention to the fact that the person possesses a cranial neuroprosthetic device.[35] Finally, such shielding would potentially block not only wireless RF attacks created by adversaries but *all* wireless RF communications; this would be impractical and even dangerous to the host's health and well-being if the implanted device requires periodic instructions communicated wirelessly from an external system in order to operator correctly (or if an external system needs to receive periodic communications from the implanted device – e.g., containing real-time medical data from the host – in order to correctly configure and apply medical treatments and ensure the host's safety and health). Indeed, in such cases, it would be imperative for a device's host to ensure that an adversary did *not* surreptitiously alter the host's clothing or provide the host with clothing that includes shielding that would disrupt the proper functioning of the host's neuroprosthetic devices.

Subcutaneous buttons that grant access to a device

Hansen and Hansen also suggest the possibility of a subcutaneous button that is implanted beneath the surface of the host's skin and which can be activated by pressing the host's body at a particular location. When the button is pressed, the IMD temporarily enters a special programming mode that disables some of its security controls and allows the device to be remotely accessed and reprogrammed (e.g., through wireless transmissions) for a specified period of time.[36] Hansen and Hansen note that such a button might be prone to being pressed accidentally, thus its location and nature would need to be carefully chosen in order to minimize such possibilities.

We would argue that while perhaps not appropriate as a sole security control, such a device might be more effectively used in conjunction with other security controls. For example, if one needed to both press the button *and* possess a particular hardware token or remove shielding from the body in

---

[35] The "tin foil hat" found within popular culture as a stereotypical tool used by paranoid individuals to protect themselves from telepathic attacks and mind control might thus – while not the most effective approach to neural defense – be an idea not entirely lacking in substance. For an analysis of the RF-shielding properties of such devices, see Rahimi et al.. "On the effectiveness of aluminium foil helmets: An empirical study" (2005). For a discussion of "psychotronics" in popular culture (as well as of supposed efforts on the part of military agencies to develop technologies that could potentially be used for remote mind control), see Weinberg, "Mind Control" (2007).

[36] See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

order to wirelessly access the implanted device, this would create greater security. Even including two different subcutaneous buttons in different parts of the body that need to be pressed simultaneously or within a certain window of time would increase security and reduce the likelihood of the device's wireless access controls being inadvertently disabled.

Another design question to be considered is whether the existence and nature of a subcutaneous button should be visible to the naked eye, visible only with the aid of particular equipment (such as an ultraviolet lamp), or wholly undetectable to outside parties. Making a button less easily detectable would decrease the changes that an adversary would discover its existence, while perhaps also making it more difficult for emergency medical personnel to notice that the host possesses an implanted neuroprosthetic device and successfully access it.

An external unit maintaining the secured state of an implanted device

Denning et al. propose a model in which the host of an implanted medical device carries a secondary, external device (which they call a "Cloaker") that controls the access that other external systems can gain to the implanted device. While they propose and consider several different variations on that theme, all of the cloaking approaches of this type share in common the fact that when the cloaking device is present, the implanted device can only be accessed by certain authorized parties; when the cloaking device is absent (or nonfunctional), the implanted device "fails open" into a state in which the implant responds to all access requests received from external systems. In the case of a medical emergency, medical personnel could access the implanted device simply by removing the cloaking device from the primary device's host.[37]

The IMD could potentially determine whether or not the external cloaking device is present by sending an "Are you there?" query to the cloaking device every time that some external system attempts to access the IMD, however Denning et al. note that this could expose the IMD to a denial of service attack in the form of a resource depletion attack that attempts to exhaust the IMD's battery simply by sending an unceasing series of access requests. Denning et al. thus suggest an alternative approach in which the IMD sends an "Are you there?" query to the cloaking device at periodic, nondeterministic intervals set by the device's designer; the designer could choose intervals that are brief enough to ensure that the IMD will fail open quickly enough in the case of a medical emergency but not so brief that the IMD's battery will be exhausted through frequent queries. Denning et al. note that one challenge for this model is to deal effectively with the possibility that an adversary could jam

[37] See Denning et al., "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security" (2008).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

the wireless communications between the IMD and cloaking device, thereby inducing the IMD to fail open into a nonsecured state in which the adversary can gain access to the implant. Another disadvantage is the fact that while the IMD's periodic "Are you there?" queries to the cloaking device may not consume large amounts of power, they do place some drain on the unit's power supply, which – as for many implantable devices – may be quite limited and difficult to replenish.

An external gateway that jams communication with the implanted device

Zheng et al. propose a model in which the host of an implanted device also wears or carries an external "gateway" device that controls access to the implant. The gateway device not only jams wireless communication and blocks transmissions (e.g., from an adversary) from reaching the implanted device, but it also impersonates the implanted device and communicates with an adversary's system whenever it detects an adversary attempting to access the implant. Because all of the adversary's access requests are being received and processes by the external gateway rather than the implant, it is not possible for the adversary to subject the implant to a resource depletion attack and exhaust its battery or otherwise disrupt its functioning by subjecting the implant to an unending series of access requests. In the case of a medical emergency, medical personnel who are treating the device's host need only locate and power off the external gateway device worn or carried by the host; as soon as the gateway has been disabled and its jamming and spoofing activities have ceased, direct wireless access to the implanted will be possible.[38] In a sense, this model is similar to the "Cloaker" approach proposed by Denning et al., however it places no drain on the IMD's battery, since the IMD does not need to send periodic "Are you there?" queries (or otherwise transmit data to) the external component. It also eliminates the possibility that an adversary could impersonate the external cloaking device and send wireless signals to the IMD that force the IMD to remain secured and inaccessible when the device's host is indeed undergoing a health emergency and medical personnel have removed the "real" cloaking device from the host's person.

Audible alerts to increase host's awareness of potential attacks

Halperin et al. note that some IMDs generate an audible alert that their host can hear when the device's battery is nearly exhausted, and they recommend that similar audible alerts be used as a supplemental security measure

[38] See Zheng et al., "A Non-key based security scheme supporting emergency treatment of wireless implants" (2014).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

for IMDs: if a device detects suspicious activity that may indicate an attack (such as a series of unsuccessful attempts by a wireless user to access the device), the device could generate an audible alert that the device's human host would hear.[39] Halperin et al. note that while such an alert would not in itself directly block an ongoing attack against the device, the fact that the device's host has been alerted to the possibility of an ongoing attack means that the host then could take specific actions (e.g., as previously instructed by the device's operator) that would directly prevent or block an attack that was in progress.

However, Hei and Du note that an audible alert might not be noticed by the device's host if the he or she were in a noisy environment (nor, we might add, if the host were asleep); they also note that a mechanism for generating an audible alert consumes electrical power and thus cannot easily be incorporated directly into an implantable device itself, insofar as power is a limited and very precious commodity for many such devices.[40]

Halperin et al. propose to avoid such power constraints by implanting a secondary device whose sole purpose is to audibly alert its human host to attacks on the primary implanted device. They have developed an implantable prototype based on the Wireless Identification and Sensing Platform (WISP) that can harvest energy from an external power source in the form of a radio signal generated by a standard UHF RFID reader; in this way, the secondary WISP device places no demands on the power supply of the primary device implanted in the host.[41] The WISP devices uses a piezoelectric element to generate an audible beep if it detects certain kinds of RF activity (such as a series of wireless access requests from an external RFID reader) that could indicate an attempt by an adversary to access the primary implanted device.

An alternative approach proposed by Halperin et al. similarly relies on the use of sound to make a device's host aware of a potential attack: they have developed a prototype implantable device that exchanges its symmetric cryptographic key with an external system using sound waves that are audible to the device's host and detectable by an external system in close proximity to the host's body but not detectible (e.g., to adversaries) at significant distances from the host's body.[42] In this way, whenever the device's host hears the relevant kind of sound generated by the implanted device, he or she knows that some external system has just submitted an access request to the implanted

---

[39] See Halperin et al., "Security and privacy for implantable medical devices" (2008), p. 37.

[40] See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011), p. 2.

[41] See Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" (2008).

[42] See Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" (2008).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

device and is receiving the cryptographic key. If that attempt is unauthorized, the host could potentially thwart it by moving away from that location and away from whatever external device was the source of the attack.

Securing a neuroprosthetic device vs. securing a neurocybernetic device-host system

A recurring theme throughout this text will be the distinction between ensuring information security for a neuroprosthetic device *per se* and ensuring information security for the larger neurocybernetic system that includes both the device and its human host. When discussing information security for neuroprosthetic devices, one must be careful to clarify whether the goal and effect of a particular security control is to strengthen the security of information contained within the device or within the larger device-host system.

For example, imagine a human being who possesses an advanced cochlear implant that records all of the person's auditory experiences and can later "play back" any part of the recording internally through the person's cochlear nerve in a way that only he or she can hear, with the playback feature activated and controlled by acts of volition within the host's mind. [43] It may be the case that the cochlear implant possesses numerous security controls that make it almost impossible for an unauthorized party to directly access the information stored within it. Such controls might include, for example, an anti-tampering mechanism that destroys the device's internal memory if the device's physical casing is removed and a biometric control integrated into the device's processor that is based on the host's unique cognitive patterns and which disables the playback feature if the device were to be transplanted into some other host's body or physically connected to another computer. In this situation, one might say that all of the recorded auditory information stored on the device's internal memory is (almost) completely secure from access by any unauthorized party. But if we look not at the physical neuroprosthetic device itself but at the larger device-host system of which it is a component, we see that the information stored in the device is in fact highly unsecure: the device's host can play back recorded information (such as a conversation that he or she had overheard) in his or her mind through a simple act of will and then easily share that information with unauthorized parties simply by repeating it aloud, writing it down, or answering parties' questions about the information.

---

[43] Regarding the possibility of such playback devices, see Merkel et al., "Central Neural Prostheses" (2007), and Robinett, "The consequences of fully understanding the brain" (2002).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

The device's host might share such information with unauthorized parties accidentally and unintentionally (e.g., sharing information about a sensitive conversation without realizing that the person with whom the information was being shared is an unauthorized party), as an intentional action performed by the host (e.g., sharing information from a damaging conversation in order to exact revenge on a disliked coworker), or under duress (e.g., as a result of severe threats, blackmail, or enticement offered by the unauthorized party).

If the developers and operators of neuroprosthetic devices wish to maximally secure information contained within their devices, they must consider not only the characteristics and performance of a device as it exists in the abstract – physically and operationally separated from its human host – but also how the device functions when integrated into the neural circuitry of a particular human host. The device-host system may demonstrate unique cybernetic, biocybernetic, and neurocybernetic characteristics (such as feedback loops and other relationships of communication and control) that are neither visible nor even extant when the device and its host are considered separately or are, in fact, disconnected from one another.

Moreover, we will also extensively consider the possibility that an attack might be launched on a neuroprosthetic device by an adversary not for purposes of compromising information stored within the device itself but for the ultimate purpose of compromising the security of information stored within the natural biological systems and cognitive processes of the device's host (e.g., within the host's memory or conscious awareness) – perhaps by undermining his or her health or safety. There is also a possibility that an adversary could render information stored on a neuroprosthetic device damaged, disclosed, or inaccessible not by directly attacking the device but by launching an attack (whether by biochemical, physical, psychological, or other means) against the device's human host.

The weakest link – now at the heart of an information system

Human beings are considered to be the weakest link in any system of information security controls:[44] not only can we make unintentional physical or mental errors in operating a system or be fooled by social engineering attacks,

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

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

we can also potentially become corrupted through greed, jealousy, resentment, lust, shame, pride, or ambition, and agree to take on an active and intentional role in disabling or bypassing our organization's security controls.[45]

With some kinds of information systems – e.g., those that are housed in physically and electronically isolated environments; are managed by a small and carefully screened team of expert personnel; contain no information that is financially, politically, or personally sensitive; and, once activated, perform their tasks in an automated manner largely devoid of direct human intervention or control – the opportunity for security vulnerabilities to be intentionally exploited by human adversaries or unintentionally trigged by human agents can be reduced to a relatively small level. With other kinds of systems that have a much higher exposure to human activity – such as systems that are physically housed in publically accessible or mobile locations; have hundreds or thousands of individuals who possess privileged access to the system; and contain highly sensitive and valuable information that is provided, altered, and deleted daily by millions of human users utilizing web-based interfaces – the threat that a system's information security will eventually be compromised by human agents acting intentionally or unintentionally can be much greater.

It is easy to see that in the case of advanced neuroprosthetic devices, a system will always possess a large and crucial human element that cannot be eliminated: namely, the fact that the device is actually integrated into the neural circuitry of a human being. In this sense, a neuroprosthetic device inherently demonstrates a unique set of vulnerabilities that are found in no other systems, whether they be supercomputers, desktop computers, laptops, mobile or wearable devices, ubiquitous computing devices in smart homes or offices, web servers, automobiles, robotic manufacturing systems, communications satellites, video game systems, or any other computerized systems or devices.

The human mind – with its emotions, cognitive biases, incomplete knowledge, uneasy mix of gullibility and suspicion, and unique values and motivations – forms a perilous and unpredictable element of any information system. And in the case of an advanced neuroprosthetic device, that mind is often permanently anchored at the very heart of the system, where it is relentlessly active 24 hours a day in influencing and perhaps even controlling the functioning of the system – where it may be able to bring about some dramatic change in the contents of an information system or some tangible

[45] For the possibiity of insider threats, see Coles-Kemp & Theoharidou, "Insider Threat and Information Security Management" (2010).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

physical action in the world simply by means of an idle thought or volition or the recalling of a hazily outlined memory.

Many kinds of advanced neuroprosthetic devices take the most dangerous and weakest possible link and embed it irrevocably at the very core of an information system which one nevertheless hopes to – somehow – make secure. Admittedly, this intimate connection between mind and machine can also possess its own unique advantages. The human mind tied to a neuroprosthetic device can display human strengths such as flexibility, intuition, the ability to correlate vast and unrelated pieces of knowledge and experience, creativity, and even faith, hope, and love – characteristics that allow a human mind not only to detect threats that a machine may be unable to recognize but also to wisely discern those rare instances when bypassing, disabling, or ignoring a security control in some particular circumstance may actually be the best (or only) way to ensure the information security of a system, individual, or organization. From the perspective of information security, integrating the neural circuitry of a human being with an electronic device can – for better or worse (or both) – bring with it not only the neurons and synapses of a human brain but also the intellectual, emotional, and even spiritual aspects of a human mind.

New kinds of information systems to be protected – or used in executing attacks

Information security experts whose goal is to develop and implement mechanisms and procedures to ensure the information security of advanced neuroprosthetic devices and their corresponding device-host systems have a clear need to learn as much as possible about the capacities and uses of advanced neuroprosthetic devices. What may be less immediately obvious is that *all* information security practitioners may need to develop at least some basic knowledge or awareness of the capacities and uses of advanced neuroprosthetic devices, insofar as such technologies provide powerful new tools by means of which attacks against all kinds of information systems – whether laptop computers, web servers, smartphones, archives of printed documents, or even human minds – can be launched and executed by sufficiently skilled adversaries.

Some adversaries may operate neuroprosthetic devices that are implanted in their own bodies. For example, a person could use an artificial eye to record secret video, an advanced cochlear implant to record conversations that are scarcely audible to a normal human ear, or an advanced virtual reality neuroprosthetic that allows him or her operate within cyberspace, sensing and manipulating it in a way that no unmodified human being could. Other adversaries might not host any neuroprosthetic devices within their own bodies,

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

but they might be able to gain unauthorized access to neuroprosthetic devices implanted in other human hosts. For example, an adversary who hacked into the artificial eye of a corporation's vice president might use the ongoing live video feed to gain access to a plethora of financially valuable business secrets that are displayed on the vice president's computer screen and are contained in a corporate computer system that is otherwise impossible to break into. An adversary could gain access to a secured facility not by tunneling into the building but by hacking into the human security guard's mnemoprosthetic implant and creating a false memory of the "fact" that the adversary is a senior staff member at the facility and should be welcomed when he arrives at the front door.

In such ways, the use of advanced neuroprosthetic devices within human societies will require not only the development of a specialized subfield of information security dedicated to securing such devices and their device-host systems but also new approaches and responses across all of the other subfields of information security, as they adapt to the existence of such new technological means for planning and executing attacks on information systems.

New possibilities for biometrics

Other researchers have suggested that one approach to creating implantable devices that are highly secure during normal circumstances but grant open access during health emergencies is to take advantage of one of the unique strengths of implantable devices: namely, their ability to draw rich, real-time biometric data from their human host. Biometrics that have been used for purposes of authentication for information systems in general (but not implantable neuroprosthetic devices in particular) include:[46]

- Facial geometry
- Ear geometry
- Hand geometry (including vascular patterns)
- Fingerprints
- Palmprints
- Retinal patterns
- Iris patterns
- Infrared thermograms of patterns of heat radiated from the face or hand

[46] See Delac & Grgic, "A Survey of Biometric Recognition Methods" (2004), and Rao & Nayak, *The InfoSec Handbook* (2014), pp. 297-303.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

- Signature and handwriting patterns
- Keystroke and typing patterns
- Gait and walking patterns
- Vocal characteristics
- Odor
- DNA

Many of these biometrics may be impractical if the designer of a neuroprosthetic device is attempting to create a security control mechanism within the device to ensure that it is still located within and being operated by its intended human host. For example, a memory implant located within its host's brain has no direct means by which to observe the iris patterns or patterns of heat radiated from the hands of its human host. However, an implanted neuroprosthetic device could potentially utilize some such biometrics if it had access to relevant biological sensory systems within its host: for example, if a sufficiently sophisticated neuroprosthetic device implanted within its host's brain had access to the optic nerve or visual cortex, it could conceivably conduct an iris scan by asking its host to stand in front of a mirror and look at the reflection of his or her own eyes. Instead of verifying that a neuroprosthetic device is still implanted in its intended host, some such biometrics could potentially be used by a neuroprosthetic device to authenticate another individual (such as a maintenance technician) who is not the device's host but who is an authorized user and who should be given access to the device's systems: for example an individual who possesses a bidirectional robotic prosthetic arm could potentially authenticate that another person is an authorized user simply by shaking the person's hand and thus detecting the person's hand geometry through touch or through optical or thermal sensors embedded in the prosthetic hand's palm or fingers.

Beyond such general-purpose biometrics, a number of biometrics have been developed or considered especially for use with implantable medical devices and are designed to take advantage of an implanted device's ability to directly access information about its host's internal biological processes. Such biometrics include:[47]

- Heart rate
- Breathing rate
- Blood glucose level
- Hemoglobin level

[47] See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), pp. 207-09.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

- Body temperature
- Blood pressure

Below we consider a number of biometrics and biometric systems that have been specifically proposed for or could conceivably be applied for use with advanced neuroprosthetic devices.

Fingerprint type, eye color, height, and iris pattern

Hei and Du have proposed a biometric-based two-level security control to allow medical personnel to access implantable medical devices during an emergency. Prior to its implantation, a key is installed on an IMD that contains information about the basic fingerprint type, eye color, and height, and a code representing the iris pattern of its human host. When emergency medical personnel attempt to remotely access the IMD using their computer, the device will first ask the personnel to enter the host's fingerprint type, eye color, and height, as an initial access control; the medical personnel can obtain all of this information by physically observing and manipulating the host, even if he or she is unconscious. As a more sophisticated control, the IMD then asks the medical personnel to take a photo of the host's iris (e.g., with a smartphone); an algorithm uses the photo to generate a code representing the iris pattern, which is then compared against the host's reference iris code stored in the IMD.[48]

Hei and Du note that such an approach would fail to provide access to legitimate medical personnel, for example, in cases in which the host's fingerprints had been damaged due to a fire or other injury or in which the host's body was trapped or positioned in such a way that the personnel could not photograph the host's eyes.

Another possible disadvantage of this approach is the fact that it is based on the presumption that authorized emergency medical practitioners are the only individuals who would have both the desire to access and control the host's IMD and the ability to gather the necessary biometric data through direct physical interaction with the host. However, it seems possible that a sufficiently motivated adversary who wishes to gain unauthorized access to the host's IMD could potentially gather all of the needed biometric data simply by downloading high-quality images of the individual from the Internet.[49]

---

[48] See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), p. 208.

[49] For an example of this sort of vulnerability and risk, see Hern, "Hacker fakes German minister's fingerprints using photos of her hands" (2014).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

The heart's interbeat interval

Cho and Lee propose a model for secure communication among implanted biosensors or between an implanted biosensor and external system that uses the interbeat interval of the host's heartbeat.[50] The advantages of using that data source as a symmetric key for secure communications include the heartbeat's relatively high level of randomness (in comparison to some other potential biometrics) and the fact that the heart's interbeat interval can be detected by devices located throughout the host's body using a variety of mechanisms (e.g., by registering electrical activity or blood pressure) and can also be detected on the external surface of the host's body but cannot easily be detected by any adversary who does not have direct physical access to the host at that moment.

Strings generated from real-time ECG signals

Zheng et al. propose an "ECG-based Secret Data Sharing (ESDS) scheme" to secure information that is being transmitted from an implanted device to an external system. Before its transmission from the implanted device, data is encrypted by the device using a key based on current biological activity that generates ECG signals that the device registers and which an external ECG is also capable of recording. After the message has been transmitted, it can be decrypted by an external system that had been using its own external ECG unit to record the host's activity at the same time and which can thus reconstruct the key.[51]

Gait and voice patterns

Vildjiounaite et al. propose a noninvasive multimodal model for securing personal mobile devices such as smartphones[52] that in principle could also be applied to implantable neuroprosthetic devices. Their approach involves utilizing a device's built-in microphone and accelerometer to gather information about both the unique gait or walking patterns of the device's host along with unique characteristics of the host's voice. After activation, the security program enters a "learning mode" for a period of a few days, during which time it records and analyzes the host's typical gait and voice patterns; if the device is able to establish suitably stable reference patterns, it then enters the "biometric authentication mode" in which it regularly compares the

---

[50] See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012).

[51] See Zheng et al., "Securing wireless medical implants using an ECG-based secret data sharing scheme" (2014), and Zheng et al., "An ECG-based secret data sharing scheme supporting emergency treatment of Implantable Medical Devices" (2014).

[52] See Vildjiounaite et al., "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices" (2006).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

gait and voice patterns that it is currently detecting against the reference patterns stored within it and – assuming that the current patterns and reference patterns match –authenticates the device's host and provides ongoing access to services.[53]

Behavior changes

Denning et al. note that one approach to securing implantable medical devices involves "patient behavior changes," in which the host of a device is asked to modify his or her behavior in some way as part of implementing a security control.[54] The sense in which Denning et al. use the phrase is broad enough to include cases in which the host's behavior change is the result or side-effect of a security control rather than the primary means by which the control is enforced. However, momentary "behavior changes" could also be used as a sort of security control to verify that a neuroprosthetic device was still being used by its intended human host. For example, a device's host might periodically receive a certain kind of signal from the device, such as a visual alert displayed in the host's field of vision, an auditory alert produced through stimulation of the auditory cortex that the host can hear but no external parties can detect, or a stimulation of the host's proprioceptive system. After receiving the signal, the host then has a limited period of time in which to perform some particular (ideally inconspicuous) behavior that the implanted device can detect – such as blinking his or her eyes in a certain pattern, making a certain sound, or moving his or her fingers in a particular way. If the device detects the required behavior, it authenticates the device's host as an authorized party and allows ongoing access to the device's services for a particular period of time.

Thoughts and memories

One model of using a user's thoughts and memories as a biometric is presented by Thorpe et al. in their proposed mechanism for utilizing "passthoughts." In the simplest such approach, an authorized user memorizes a brief password, thereby storing it as a memory within his or her mind. When the user wishes to access a system, the system displays a random sequence of highlighted letters, and whenever the highlighted character happens to be the next character in the user's password, the user's brain generates a P300 potential spike (or a positive potential that occurs roughly 300 milliseconds

---

[53] Vildjiounaite et al., "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices" (2006), p. 197.

[54] Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010) p. 919.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

after the notable event) that can be detected by the system using an EEG or other device. Thorpe et al. note that such a pass-thought need not involve a text string; it could alternatively involve the use of "pictures, music, video clips, or the touch of raised pin patterns" or anything else that a person is capable of remembering and which the system is capable of displaying or presenting.[55] However, at its heart such a "pass-thought" mechanism is essentially based on the use of a password as traditionally understood; the main difference is that rather than typing the password on a keyboard or speaking it aloud, an authorized user "enters" the components of the password through interaction with a brain-computer interface that utilizes a device such as an EEG. Such a system thus displays many similarities with traditional password-based systems, insofar as an authorized user might forget his or her pass-thought (e.g., if it had been a long time since the user had last attempted to access the system); similarly, a user could be issued a new temporary pass-thought by a system's administrator (e.g., by displaying the contents of the pass-thought on a screen and asking the user to remember it) and the user could change the pass-thought to something new of his or her own choosing.

One can imagine other more sophisticated kinds of security controls based on cognitive processes such as thought and memory that are more exotic and which from an operational perspective have less in common with traditional password-based systems. For example, the same word (e.g., "home" or "mother" or "cat") or image (e.g., that of a wooded lake or a birthday cake) displayed to different individuals will generate different associations and the recall of different memories within each of the individual's mind because of the unique contents of each person's memories and life experience. The contents and internal interrelationships of such mental semantic networks could potentially be used as a form of authentication that cannot easily be lost, stolen, or spoofed, insofar as they are not directly accessible to parties outside of the mind that possesses them, and a human being cannot adequately understand and describe the nature and contents of his or her mental semantic networks even if he or she were intentionally attempting to do so (e.g., because the person were being subjected to threats or blackmail).

DNA

The use of DNA for verifying the identity of individuals has traditionally been limited to forensic applications rather than biometric access control for information systems, due to the fact that technologies have not yet been developed allowing simple real-time analysis and matching of a DNA sample with a reference pattern; however if such technologies were to someday be developed, DNA could potentially prove to be the most reliable of all biometrics (with some rare limitations, such as the case of identical twins whose

[55] See Thorpe et al., "Pass-thoughts: authenticating with our minds" (2005).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

DNA is indistinguishable).[56] Because of the uniqueness of DNA and its potentially high reliability as a biometric, some information security experts have suggested that it could someday be utilized as a biometric means for an implanted neuroprosthetic device to verify that it is operating within its intended human host.[57]

Spurred by ongoing advances in bionanotechnology, biomolecular computing, and related fields, DNA could also someday be used as a biometric or authenticator in other ways. For example, in the case of a neuroprosthetic device that is composed of synthetic biological materials, other implanted systems could analyze the device's DNA in order to verify its origins and authenticate it (e.g., locating a particular sequence of DNA within the device's genetic material in order to confirm that the device was created by the intended authorized manufacturer and was not an unauthorized growth or biohack that had somehow been cultivated within the device's host through an adversary's introduction of engineered viruses, surgical nanorobots, or other unauthorized agents).

Multiple devices that have been implanted in the same host and which form a system could also potentially communicate with one another through their production of different viruses or biological material that are released into the host's bloodstream and travel between devices, e.g., utilizing the engineered virus's DNA or RNA as a data-storage mechanism for transmitting messages between the implanted devices and allowing one device to verify that the other devices are still present and functioning within the host's body. An electronic or biological neuroprosthetic device could also use DNA, for example, as a means of deploying and storing encryption keys for use in authenticating or being authenticated by other systems.[58]

Organismic continuity (or a continual "liveness scan")

Qureshi notes that some kinds of biometric traits can be spoofed by presenting the biometric reader with an artificial construct of some sort that is not actually part of the authorized party's living organism but which nonetheless presents patterns that mimic those of the person's organism.[59] Thus some kinds of fingerprint readers could potentially grant access to an adver-

---

[56] Delac & Grgic, "A Survey of Biometric Recognition Methods" (2004), p. 188.

[57] For example, the question of whether this might be a feasible approach has been posed by Pająk (2015).

[58] For a discussion of the possibilities of using DNA as a mechanism for the storage of data, see Church et al., "Next-generation digital information storage in DNA" (2012).

[59] See Qureshi, "Liveness detection of biometric traits" (2011).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

sary if the adversary presented a silicon "finger" whose surface texture replicated the fingerprint pattern of an authorized user, and some kinds of iris scanners could potentially be fooled if presented a high-quality photograph of an authorized user's iris. Qureshi notes that one way to prevent such spoofing is to incorporate mechanisms for "liveness detection" which verify that the presented biometric was actually being generated by a living organism.

For example, adding pulse and moisture detection capabilities to a fingerprint scanner can help the scanner to ensure that a presented biometric is being provided by a living finger and not a rubber replica, and an iris scanner could instruct its user to blink at certain moments, which induce predictable changes in the size of a living iris but not in a photographic replica.[60]

While helpful, such liveness detection is not foolproof. Even if an adversary were to possess sufficiently sophisticated genetic engineering and bioengineering technologies, it would generally not be possible for an adversary to directly "grow" a living organ or body part capable of fooling a biometric scanner: for example, it is not possible to generate a replica of a human being's fingerprint or iris pattern simply by obtaining a sample of the person's DNA and attempting to culture a cloned finger or eyeball, since an individual's fingerprints and iris patterns are shaped by many environmental factors beyond simple genetics. However, if the details of an authorized user's fingerprints or iris pattern were known, a living replica could perhaps be created through other means – such as using a combination of nanotechnology and biotechnology to sculpt, reshape, or otherwise reengineer the finger or iris of an unauthorized living being so that its visible patterns sufficiently matched those of the authorized target.

However, in principle the concept of liveness detection could be applied to prevent such attacks and ensure that an implanted neuroprosthetic device is not only being accessed by *a* living being who displays certain characteristics but that it is being accessed by *the same living being* in whom it was originally implanted. For example, imagine that immediately upon its implantation in a human host, a neuroprosthetic device begins a continual, ongoing "liveness scan" designed to ensure that the device is implanted in a living host – for example, by monitoring brain activity. As long as the process of scanning is reliable and uninterrupted, then as long as the scan has shown that from the moment of the device's implantation up to the present moment the monitored biological activity has continued without ceasing, then the device's software could be confident that the device is not only implanted within some living organism but within the organism of its original human host.[61]

---

[60] Qureshi, "Liveness detection of biometric traits" (2011), pp. 294-95.

[61] Such a model assumes that extracting the implant and transferring it to another living host

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Such a biometric security control based on the detection of "organismic continuity" could be used, for example, to automatically disable – or delete the stored contents of – an implanted neuroprosthetic device upon the death of its human host or the cessation of particular brain activity within the host. Care would need to be given to the design of such systems to ensure that a neuroprosthetic device did not erroneously deactivate itself and cease to operate cease in cases in which its host had, for example, suffered a heart attack or stroke or entered a coma when such a termination of functionality was not the intention of the device's designer, manufacturer, or operator.

Nontraditional computing platforms: from biomolecular computing and neural networks to nanorobotic swarms

When compared to conventional information systems such as desktop computers, laptops, and smartphones, an advanced neuroprosthetic device may be more likely to possess nonstandard, non-electronic components and to utilize nontraditional computing processes and formats. In the case of conventional computers, there is a decades-long history of design ingenuity, trial, error, and consumer feedback that has generated a body of experience and best practices allowing the efficient development and manufacturing of very powerful devices that utilize technologies such as silicon-based microprocessors, nonvolatile memory based in magnetic discs or flash memory, and computer programs constituting sets of instructions that can be loaded and executed by a central processing unit.

When developing new mass consumer electronics devices, it often makes more business sense for manufacturers to keep the cost and complexity of manufacturing processes at a minimum by designing devices that utilize well-established computing technologies while simultaneously attempting to advance those computing technologies in a way that enhances existing performance and capacities in an incremental manner. When designing a next-generation mass-market smartphone intended for consumer release next year, it would most likely be seen as an unnecessarily exotic (and practically and economically unfeasible) approach for a manufacturer to attempt to build the device's internal computer on a platform utilizing as biomolecular computing, quantum computing, or physical neural networks.

---

could not be accomplished without at least a momentary break in the relevant recorded biological activity by the device; it also assumes that the device's design and structure are such that the recorded biological activity must actually be generated by biological activity occurring in biological material directly adjacent to the device and not, for example, spoofed through a targeted wireless transmission of certain electromagnetic radiation.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Advanced neuroprosthetic devices, on the other hand, already inherently incorporate and rely on at least some highly "exotic" and "nonstandard" computing components and processes, insofar as they must integrate both physically and operationally with the biological structures and neural circuitry of their human host. When considering information security for advanced neuroprosthetic devices, one cannot assume that a neuroprosthetic device will be a traditional computing device – with traditional kinds of components, architectures, memory systems, and ways of gathering and processing information to generate actions and output – that has simply been implanted into the body of a human host.

While some advanced neuroprosthetic devices might indeed resemble a smartphone that has just been miniaturized and implanted in a human body, other neuroprosthetic devices might scarcely be recognizable as computers – or even technological devices. Neuroprosthetic devices that perform the processing of information by means of a physical neural network might be partially or fully constructed from biological materials and may be integrated into the body of their host in a way that makes it difficult to discern – both structurally and operationally – where the host ends and the device begins. Information security might involve protecting a neuroprosthetic device not only against computer viruses but against biological viruses, as well. In order to avoid invasive surgery that could damage a human host's brain, other neuroprosthetic devices might consist of a swarm of nanorobots that have been designed to be capable of crossing the blood-brain barrier and which are introduced into the host's bloodstream and find their way to the correct location in the brain, where they work together to stimulate (or are stimulated by) the brain's natural interneurons in particular ways, even while retaining their physically diffuse structure.[62]

The possibility that neuroprosthetic devices might take such forms creates unique issues and considerations for information security. On the one hand, the use of nontraditional components, structures, and computing methods may render a neuroprosthetic device more secure, because common kinds of attacks that are often effective against conventional computers and information systems may be ineffective or even wholly inapplicable in the case of neuroprosthetic devices. On the other hand, the use of nontraditional elements may mean that the designers, manufacturers, operators, and hosts of neuroprosthetic devices cannot rely on the vast body of information security knowledge and best practices that have been developed over decades for securing conventional computer systems, because many of those information security strategies, mechanisms, and techniques may also be ineffective or inapplicable in the case of neuroprosthetic devices.

---

[62] See Al-Hudhud, "On Swarming Medical Nanorobots" (2012).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Technology generating posthuman societies and posthuman concerns

Philosophers of technology have given much thought to the transformative effects that technology can play in the lives of human beings, either as a means of liberation and self-fulfillment or as a source of oppression and dehumanization.[63] Even technologies such as desktop computers and email – which interface with the human mind in only limited and indirect ways – have resulted in major psychological, social, and cultural impacts among the human beings who use them.[64] However, advanced neuroprosthetic devices have the potential to reshape human psychological, social, and cultural realities – and even challenge many popular notions of what it means to be "human" – in ways greater and more powerful than those demonstrated by previous generations of technology. In this regard, advanced neuroprosthetics are similar to other technologies such as genetic engineering, artificial intelligence, social robotics, virtual reality, and nanotechnology that have the potential to reshape human existence in such a way that the resulting kinds of beings, systems, and organizations might best be described as "posthuman."[65]

Already "cyborg-cyborg interaction" is becoming a fundamental aspect of society,[66] and genetic engineering may accelerate trends of cyberization by further enhancing the ability of the human body to interface at a structural level with implanted or external technological systems. Increasingly businesses and other organizations comprise "cybernetic teams" whose human and artificial members "cooperate as teammates to perform work."[67] Indeed,

---

[63] For a discussion of such questions in the context of human augmentation and neuroprosthetics, see Abrams, "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault" (2004); Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011); Erler, "Does Memory Modification Threaten Our Authenticity?" (2011); Tamburrini, "Brain to Computer Communication: Ethical Perspectives on Interaction Models" (2009); and Schermer, "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction" (2009).

[64] For example, see Fox & Rainie, "The Web at 25 in the US: Part 1: How the Internet Has Woven Itself into American Life" (2014), and Shih, "Project time in Silicon Valley" (2004).

[65] For the convergence of nanotechnology, biotechnology, information technology, and cognitive science (or "NBIC" technologies), see Gordijn, "Converging NBIC Technologies for Improving Human Performance" (2008); for a deeper exploration of such technologies' relationship to posthumanism and posthumanity, see Birnbacher, "Posthumanity, Transhumanism and Human Nature" (2008). For aspects of posthumanism that extend beyond technology, see Miah, "A Critical History of Posthumanism" (2008).

[66] See Fleischmann, "Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI" (2009).

[67] See Wiltshire et al., "Cybernetic Teams: Towards the Implementation of Team Heuristics in HRI" (2013); Bradshaw et al., "From Tools to Teammates: Joint Activity in Human-Agent-Robot

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

the increasing virtualization of our relationships means that we will regularly interact with coworkers, customers, and suppliers as digital avatars in virtual environments, without knowing (or perhaps caring) whether the entity on the other end of a conversation is a human being, social robot, or AI program.[68] Neuroprosthetics will allow for increasingly intimate forms of communication that do not involve physical face-to-face interaction but are instead mediated by technology, thereby facilitating the development of new kinds of posthuman interpersonal relationships and social structures.[69]

Such powerful new technologies are introducing a "radical alterity" that challenges not only the traditional values of humanism but also our most fundamental understanding of the limits and possibilities of what it means to be human, in a time when philosophical and ethical frameworks that "privilege reason, truth, meaning, and a fixed concept of 'the human' are upended by digital technology, cybernetics, and virtual reality."[70] A variety of responses to such technologies has emerged. For example, on the one hand, scientists and philosophers identifying themselves as **transhumanists** accept the basic humanistic principles of anthropocentrism, rationality, autonomy, progress, and optimism about the future of humanity, while actively working to employ science and technology in an effort to control and accelerate the transformation of the human species in ways that traditional biological evolution does not allow. Such thinkers advocate the use of genetic engineering, cybernetics, and nanotechnology to create a supposedly more meaningful, more transcendent, "enhanced" form of human existence. In this sense, their philosophy can be understood not as "anti-humanism" but as their expression of a unique form of "ultra-humanism."[71]

On the other hand, there is a diverse group of **posthumanistic** thinkers who agree that new forms of sentient and sapient existence are emerging, spurred on by the world's technological advances; however, these thinkers reject transhumanism's anthropocentric and humanistic focus. Instead, posthumanists argue that the future will include many different sources of intelligence and agency that will create meaning in the universe through their networks and relations:[72] such entities might include "natural" human beings,

---

Teams" (2009); and Flemisch et al., "Towards a Dynamic Balance between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations" (2012).

[68] See Grodzinsky et al., "Developing Artificial Agents Worthy of Trust..." (2011).

[69] See Fleischmann, "Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI" (2009), and Grodzinsky et al., "Developing Artificial Agents Worthy of Trust..." (2011).

[70] See Gunkel & Hawhee, "Virtual Alterity and the Reformatting of Ethics" (2003).

[71] See Ferrando, "Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations" (2013).

[72] See Ferrando, "Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

genetically engineered human beings, human beings with extensive cybernetic and neuroprosthetic augmentation, human beings who spend most or all of their time dwelling in virtual realities, social robots, artificially intelligent software, nanorobot swarms, and sentient networks.

Thinkers like Bostrom[73] are generally enthusiastic about the transhuman potential of technologies like advanced neuroprosthetics to "liberate" humanity, allowing us to transcend our previous physical and cognitive limitations and spark the evolution of higher forms of human existence. Following paths pioneered by Habermas and Horkheimer, other scholars are more pessimistic about the anticipated impact of such transformative technologies, suggesting that while the exact impact of such technologies cannot be predicted in advance, they are more likely to spur social fragmentation and inequality, a reduction in human autonomy and meaning, and the oppression – or in its extreme form, even destruction – of humanity at the hands of its technological creation.[74]

In a sense, then, questions about the information security of advanced neuroprosthetic devices and device-host systems should be considered in a broader context relating to human societies and the human species: advanced neuroprosthetic devices should be developed (or, if necessary, *not* developed) in such a way that will ensure not only that individual persons' information security can be protected – but that a humanity and human species can continue to exist whose members are able to generate, use, and exchange information and hope for the protection of its security.

Human autonomy, authenticity, and consciousness: risk management and the possibility of ultimate loss

Materialisms: Differences and Relations" (2013).

[73] See Bostrom, "Why I Want to Be a Posthuman When I Grow Up" (2008).

[74] As Abrams has noted, yet another group of thinkers takes an extreme position, arguing that while humanity's twilight and replacement by artificial beings such as social robots or artificial superintelligences is indeed inevitable, it is in fact a natural and desirable step in the evolution of intelligent life on earth. See Abrams, "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault" (2004), and Edgar, "The Hermeneutic Challenge of Genetic Engineering: Habermas and the Transhumanists" (2009). The struggle between those who wish to build a utopian world and manipulate the very nature of reality through the technological augmentation of human beings and those who shun such technologies and instead wish to build a utopia and reshape reality by means of a spiritual or mystical "augmentation" of human beings is a theme that has been well explored within literature, film, and popular culture. For an analysis of one such dichotomy, see Szczepocka, "Konflikt sprzecznych utopii jako główny problem gry fabularnej 'Mag: Wstąpienie'" (2015).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

Advanced neuroprosthetics thus force us to ponder the future existence and nature of humanity in a way that is elicited by other technologies such as nuclear weaponry or genetic engineering but is not found, for example, with technologies such as desktop computers or even self-driving automobiles. Nevertheless, from the perspective of information security, the primary focus with regard to advanced neuroprosthetic devices is typically very much the technology's impact on and use by particular human beings. And through their interaction with a human being's neural circuitry, many advanced neuroprosthetic devices have the potential to reshape and transform an individual life in ways that are incredibly powerful – and can be either beneficial or harmful.

One of the gravest (and most unique) concerns that an information security professional must consider with regard to neuroprosthetic devices is the impact that they might have on the autonomy, authenticity, and conscious awareness of their human host.[75] Researchers have found, for example, that some human beings who have utilized neuroprosthetic devices for deep brain stimulation in order to treat conditions such as Parkinson's disease have reported feelings of reduced autonomy and authenticity: some such individuals find it impossible to know any longer whether "they" are actually the ones responsible for their thoughts, desires, emotions, and decisions, or whether these mental phenomena are being influenced, controlled, or even created by the electrodes firing deep within their brains.[76]

It is possible to imagine a concrete outcome of the use of particular kinds of (poorly designed or implemented) neuroprosthetic devices which – from the perspective of their human hosts – would produce not only harm but the

---

[75] For an exploration of the ways in which the implantation and use of advanced neuroprosthetic devices (and the accompanying process of "cyberization" of the devices' human hosts) can contribute to a new form of personal identity for a device-host system that fuses both biological, cultural, and technological elements, see Kłoda-Staniecko, "Ja, Cyborg. Trzy porządki, jeden byt. Podmiot jako fuzja biologii, kultury i technologii" (2015). For a discussion of the significance of the physical boundaries of a human organism and the ways in which technologies such as implantable neuroprosthetics can impact cognitive processes and the "moral sense of person" vs. "the notion of person as a subject of experiences," see Buller, "Neurotechnology, Invasiveness and the Extended Mind" (2011). For a philosophical analysis of "threats to personal autonomy" posed by brain-machine interfaces, see Lucivero & Tamburrini, "Ethical Monitoring of Brain-Machine Interfaces" (2007). Questions of personal identity and authenticity are explored by Schermer, "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction" (2009).

[76] See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011), and Berg, "Pieces of Me: On Identity and Information and Communications Technology Implants" (2012). It should be noted that Kraemer explains that other users of neuroprosthetics for deep bran stimulation report precisely the opposite experience: they feel as though the neuroprosthetic devices have *restored* their autonomy and given them increased authenticity as – for the first time in years – they are in control of their bodies once again.

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

termination of their personal identity and annihilation of their existence as a human subject within the world. For example, a mnemoprosthetic implant that is designed to enhance its users' memory capacities but which causes many of its users to enter a coma or vegetative state would be legally and ethically impermissible – not to mention being counterproductive from an information security perspective, insofar as it would render the information contained within a user's mind unavailable even to that user himself or herself.

Arguably, though, an even worse scenario would be that of a neuroprosthetic device that permanently destroys the autonomy, consciousness, personal identity, continuity of sapient self-awareness, and metavolitionality (or conscience) of its human host – in other words, that obliterates the "essence" of what makes the person human – but that does so in such a way that this destruction is not detectable to other human beings.

For example, consider an extremely sophisticated neuroprosthetic device consisting of a vast network of nanorobotic components that occupy interstitial spaces within the brain and are designed to support the synaptic activity of individual neurons.[77] Imagine that – in a manner that may not be recognized or understood even by the device's designers – this neuroprosthetic device does not actually "support" the natural synaptic activity of the brain's biological neurons but instead controls or replaces it. The physical synaptic connections between neurons (and thus their communication) are disrupted and replaced by connections between the nanorobotic "pseudoneurons." The person's physical body can still react to environmental stimuli, walk, smile, and even engage in meaningful conversations with family or friends – but in fact, the person's conscious awareness has been eliminated and the person has undergone a sort of "brain death;" all of the outward physical activity is simply being orchestrated by the extremely sophisticated processes of the artificial neural network or computer program that controls the nanorobotic system and which causes it to stimulate particular motor neurons at a particular time in order to generated desired motor behaviors. In effect, the person's body has become a sort of neurocybernetic "zombie," a mindless puppet controlled by the puppeteer of the neuroprosthetic device.[78]

---

[77] Such technologies have been proposed by some transhumanists as a possible path toward "mind uploading." See Koene, "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation" (2012); Proudfoot, "Software Immortals: Science or Faith?" (2012); Pearce, "The Biointelligence Explosion" (2012); Hanson, "If uploads come first: The crack of a future dawn" (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990) for a discussion of such issues from various perspectives.

[78] Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans,

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

There are some transhumanists (e.g., proponents of the idea of "mind uploading") who might argue that such a device would not truly destroy the consciousness or essence of its human host – and that even if it did, they would be willing and even eager to transform their own bodies through the use of such a device, insofar as it might provide a bridge that would allow them to "transfer" their memories and patterns of mental activity into a robotic or computerized body that would essentially allow them, as they see it, to live forever. There may indeed be some human beings who would be happy to imagine that at the cost of destroying their own embodied consciousness, a biomechanical automaton or robot could be created that would go about its activities in the world, replicating the habits and behaviors and continuing the social relationships of the person who had served as its template, simulating the person's emotions and recreating his or her memories in the way that a video recording recreates some filmed event. But for most human beings, a neuroprosthetic device that destroys their embodied conscious awareness would be considered an absolutely impermissible – and, indeed, lethal – outcome, regardless of whatever other effects it might yield.

A dilemma for information security professionals (and the designers and operators of neuroprosthetic devices) is that in principle it may sometimes be impossible to know what effect a neuroprosthetic device is truly having on the cognitive processes – and especially, on the lived conscious experience – of its human host. If the human host of an experimental neuroprosthetic device asserts that the implantation and activation of the device has in no way harmed or diminished his or her sapience and conscious awareness, this could mean that the device has indeed had no such effect – or that it has destroyed or "imprisoned" the host's conscious awareness and agency in such a way that the source behind that statement was not the human being but the agency of the neuroprosthetic device itself. It is possible to imagine a situation in which the conscious awareness and autonomous agency of the human host might still exist – but no longer has the ability to control the motor systems of its body and alert the outside world to the fact that it still exists and is essentially "trapped" helplessly within a body whose sensorimotor systems are now controlled by the neuroprosthetic device.[79] Although more sophisticated forms of neural scanning and imaging, computer simulations of the effects of neuroprosthetic devices, research into artificial intelligence, and

---

Robots, and Hybrid Intelligences" (2015); Gladden, "'Upgrading' the Human Entity..." (2015).

[79] In a sense, such an occurrence would be the (unfortunate) mirror opposite of those positive situations in which a neuroprosthetic device provides the only means of communication with the outside world for locked-in patients who are completely paralyzed yet fully conscious, including those suffering from ALS, stroke, or traumatic brain injury. For a discussion of such positive cases, see Donchin & Arbel, "P300 Based Brain Computer Interfaces: A Progress Report" (2009).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

philosophical thought experiments may be able to provide one with reasonable grounds for suspecting (or doubting) that such a situation is possible, it may be impossible to definitively exclude the possibility if there are no independent means for settling the question outside of the host's own internal conscious experience (or lack thereof).

However remote they might be, such possibilities create particular challenges for risk management, insofar as one must grapple with the risk of an occurrence whose probability of being realized appears incredibly small (but which, in fact, cannot be reliably determined) and whose nightmarish effect on the device's host would, if realized be lethal – if not worse. While philosophers and other researchers have begun to seriously debate such issues (especially with regard to the technological and ontological feasibility of mind uploading[80]), deeper exploration of such issues from ontological, psychological, ethical, legal, and even theological perspectives is required.[81]

A growing nexus of information security, medicine, biomedical engineering, neuroscience, and cybernetics

One aspect of information security highlighted especially by our consideration of advanced neuroprosthetic devices is the growing relationship of information security to fields such as medicine, biomedical engineering, and neuroscience – and the importance that the knowledge developed in these fields will have for shaping the future of information security.[82]

It is already the case that information security is a transdisciplinary field in which personnel must not only be experts in computer hardware and software but must also have knowledge of fields such as psychology, finance, law, and ethics. However, the growing use of neuroprosthetic devices will mean that information security personnel will also need to possess at least basic

---

[80] See Koene, "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation" (2012); Proudfoot, "Software Immortals: Science or Faith?" (2012); Pearce, "The Biointelligence Explosion" (2012); Hanson, "If uploads come first: The crack of a future dawn" (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990).

[81] For a discussion of many ethical issues relating to neuroprosthetics, see Iles, *Neuroethics: Defining the Issues in Theory, Practice, and Policy* (2006). For an explicit consideration of ethical issues in light of information security concerns (and the possibility that adversaries could potentially wish to gain access to neuroprosthetic devices), see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009). For theological and spiritual issues relating to neuroprosthetic devices, see Campbell et al., "The Machine in the Body: Ethical and Religious Issues in the Bodily Incorporation of Mechanical Devices" (2008).

[82] For the increasingly inextricable connections between medical devices and information technology, see Gärtner, "Communicating Medical Systems and Networks" (2011).

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

knowledge about the biological and neuroscientific aspects of such devices. For some large organizations, it may even be desirable and feasible to add to their information security teams physicians, neuroscientists, and biomedical engineers who can work with the other team members to ensure, for example, that any information security mechanisms or practices that the organization implements in relation to its employees' neuroprosthetic devices do not result in biological or psychological harm to the employees. Such medical expertise would also be necessary in order for information security personnel to design safe and effective countermeasures that can be employed against adversaries who possess their own neuroprosthetic devices and attempt to employ them to carry out acts of illicit surveillance or corporate espionage against the company. By employing a knowledge of biology, biomedical engineering, and neuroscience, an organization's information security personnel could develop security controls and countermeasures that neutralize such threats without causing biological or psychological injury to the suspected adversaries for which the company and its information security personnel could potentially be legally and ethically responsible and financially liable.[83]

One challenge that arises in attempting to link information security with medicine is that the two fields utilize different vocabularies and conceptual frameworks: information security is grounded largely in the theoretical framework of computer science while medicine is rooted in that of biology and chemistry. In addressing this challenge, it may be helpful to build on the field of cybernetics, which was founded to provide precisely the sort of transdisciplinary theoretical framework and vocabulary that can be used to translate insights between all of the fields that study patterns of communication and control – whether it be in machines, living organisms such as human beings, or social systems.[84]

Alongside the many existing manifestations of cybernetics (found in subdisciplines such as biocybernetics, neurocybernetics, and management cybernetics) it may be useful to envision a sort of "celyphocybernetics"[85] that sees the human brain, its surrounding body, and any neuroprosthetic devices, implantable computers, and other internal or external technological systems that are integrated into the body as together forming a single physical "shell" for the human mind that possesses that body. The human brain, body, and technological devices together constitute a system that receives information from the external environment, processes, stores, and utilizes information

---

[83] For a related discussion regarding questions about the legality and ethicality of undertaking offensive countermeasures against botnets, see Leder et al., "Proactive Botnet Countermeasures: An Offensive Approach" (2009).

[84] See Wiener, *Cybernetics* (1968).

[85] From the Ancient Greek *κέλυφος*, meaning 'shell,' 'sheath,' 'husk,' or 'pod.'

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

circulating within the system, and transmits information to the external environment, thereby creating networks of communication and control. In such a model, information security experts, physicians, and biomedical engineers would thus share the single task of ensuring the secure, productive, and effective functioning of this entire information system that may contain both biological and electronic components – with that common goal only being achievable if all of the expert personnel involved succeed in fulfilling their unique individual roles.

The need for new conceptual frameworks: ontologies, typologies, and protocols for information security for neuroprosthetics

Thanks to decades of tireless visionary labor by researchers and practitioners, there now exists a coherent body of knowledge and best practices relating to information security for computerized information systems that is well-developed and battle-tested and which is being continually refined to deal with new kinds of threats. While those experts who will strive to provide information security for advanced neuroprosthetic devices will be able to ground their efforts in the existing practice of information security for computerized information systems, that general body of knowledge will, on its own, prove to be an inadequate source and guide for their efforts – because advanced neuroprosthetic devices are not simply computerized information systems. In many cases, an advanced neuroprosthetic device simultaneously possesses at least three different natures: it combines in a single device 1) a computerized information system with 2) an implantable medical device and 3) a posthuman technology that has the potential to transform the mind of its human host and radically reshape its user's relationship with his or her own mind and body, with other human beings, with technological systems, and with the external environment as a whole.

Taking into account all of the issues that we have considered earlier in this chapter, it becomes apparent that practices and mechanisms designed to protect the information security of generic computerized information systems are insufficient – if not irrelevant or, in some cases, even counterproductive – when it comes to protecting the information security of advanced neuroprosthetic devices and their device-host systems.[86] As a result, many existing

[86] Regarding, e.g., the need for new regulatory frameworks relating to implanted ICT devices, see Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012). For an example of the complexities involved with determining

*Chapter 3, "Critical Challenges in Information 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. 59-103.*

neuroprosthetic devices do not incorporate adequate security controls and do not sufficiently protect the privacy of their human hosts and users.[87]

We would argue that in order to implement robust and effective approaches for advancing the information security of advanced neuroprosthetic devices as information systems, medical devices, and transformative posthuman technologies, new conceptual frameworks will first need to be explicitly developed. Such frameworks include **device ontologies** that help one to identify and describe the relevant characteristics of a neuroprosthetic device in a systematic manner; **typologies** that use the ontologies to categorize different neuroprosthetic devices into groups that possess similar relevant characteristics; and neuroprosthetic security **protocols** that define specific device characteristics and operational practices that should be implemented in particular circumstances, based on the needs of a device's host and operator and the broader context of the device's use (including legal, ethical, and organizational considerations). Throughout the remainder of this book we will propose and explore several such frameworks. While they are designed primarily to address the unique circumstances of advanced neuroprosthetic devices, they may also yield insights that can be adapted for promoting the information security of a broader array of future "neurotech" and its human users.

---

which regulations and standards apply to which kinds of medical systems and devices, see Harrison, "IEC80001 and Future Ramifications for Health Systems Not Currently Classed as Medical Devices" (2010). For the inadequacy of traditional information security frameworks as applied to e-healthcare in general, see Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010).

[87] See Tadeusiewicz et al., "Restoring Function: Application Exemplars of Medical ICT Implants" (2012).

Chapter 3, "Critical Challenges in Information 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. 59-103.

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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 3, "Critical Challenges in Information 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. 59-103.*

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.