Chapter Seven

Detective Security Controls for Neuroprosthetic Devices and Information Systems

Abstract. This chapter explores the way in which standard detective security controls (such as those described in *NIST Special Publication 800-53*) become more important, less relevant, or significantly altered in nature when applied to ensuring the information security of advanced neuroprosthetic devices and host-device systems. Controls are addressed using an SDLC framework whose stages are (1) supersystem planning; (2) device design and manufacture; (3) device deployment; (4) device operation; and (5) device disconnection, removal, and disposal.

Detective controls considered include those relating to the establishment of an integrated InfoSec security analysis team; use of all-source intelligence regarding component suppliers; integrity indicators; designing the capacity to detect medical emergencies; integrated situational awareness; establishment of account usage baselines; general monitoring and scanning; auditing of events; threat and incident detection; and proactive detection and analysis methods.

Introduction

In this chapter, we explore a range of standard detective security controls for information systems and identify unique complications that arise from the perspective of information security, biomedical engineering, organizational management, and ethics when such controls are applied to neuroprosthetic devices and larger information systems that include neuroprosthetic components. The text applies such security controls without providing a detailed explanation of their basic nature; it thus assumes that the reader possesses at least a general familiarity with security controls. Readers who are not yet acquainted with such controls may wish to consult a comprehensive catalog such as that found in *NIST Special Publication 800-53, Revision 4,* or *ISO/IEC 27001:2013*.[1]

[1] See *NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations* (2013) and *ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements* (2013).

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Approaches to categorizing security controls

Some researchers classify controls as either **administrative** (i.e., comprising organizational policies and procedures), **physical** (e.g., created by physical barriers, security guards, or the physical isolation of a computer from any network connections), or **logical** (i.e., enforced through software or other computerized decision-making).[2] Other sources have historically categorized controls as either **management**, **operational**, or **technical** controls. As noted in the previous chapter, in this volume we follow the lead of texts such as *NIST SP 800-53*,[3] which has removed from its security control catalog the explicit categorization of such measures as management, operational, or technical controls, due to the fact that many controls reflect aspects of more than one category, and it would be arbitrary to identify them with just a single category. We instead utilize a classification of such measures as **preventive**, **detective**, or **corrective and compensating** controls. The previous chapter considered the first type of control; this chapter investigates the second type; and the subsequent chapter will explore the third and final type.

Role of security controls in the system development life cycle

The detective controls discussed here are organized according to the stage within the process of developing and deploying neuroprosthetic technologies when attention to a particular control becomes most relevant. These phases are reflected in a system development life cycle (SDLC) whose five stages are (1) supersystem planning; (2) device design and manufacture; (3) device deployment in the host-device system and broader supersystem; (4) device operation within the host-device system and supersystem; and (5) device disconnection, removal, and disposal.[4] Many controls relate to more than one stage of the process: for example, the decision to develop a particular control and the formulation of its basic purpose may be developed in one stage, while the details of the control are designed in a later stage and the control's mechanisms are implemented in yet a further stage. Here we have attempted to locate a control in the SDLC stage in which decisions or actions are undertaken that have the greatest impact on the success or failure of the given control. This stage-by-stage discussion of detective controls begins below.

[2] Rao & Nayak, *The InfoSec Handbook* (2014), pp. 66-69.

[3] See *NIST SP 800-53* (2013).

[4] Various approaches to defining the stages of an SDLC for an information system involving neuroprosthetic components are reviewed in Gladden, "Managing the Ethical Dimensions of Brain-Computer Interfaces in eHealth: An SDLC-based Approach" (2016).

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

SDLC stage 1: supersystem planning

The first stage in the system development life cycle involves high-level planning of an implantable neuroprosthetic device's basic capacities and functional role, its relationship to its human host (with whom it creates a biocybernetic host-device system), and its role within the larger 'supersystem' that comprises the organizational setting and broader environment within which the device and its host operate. The development of security controls in this stage of the SDLC typically involves a neuroprosthetically augmented information system's designer, manufacturer, and eventual institutional operator.

A. Establishment of an integrated InfoSec security analysis team

While many protective controls are relevant in the planning stage of the SDLC, only one detective control sees its critical moment occur during that stage: the establishment of an integrated InfoSec security analysis team that can detect and analyze vulnerabilities, threats, and incidents that occur throughout the remaining stages of the SDLC. In the case of advanced neuroprosthetic devices, an integrated information security analysis team may need to incorporate not only typical members such as "forensic/malicious code analysts, tool developers, and real-time operations personnel"[5] but potentially also biomedical engineers, biologists, neuroscientists, psychologists, biocyberneticists, and implantation surgeons.[6]

SDLC stage 2: device design and manufacture

The second stage in the system development life cycle includes the design and manufacture of a neuroprosthetic device and other hardware and software that form part of any larger information system to which the device belongs. The development of security controls in this stage of the SDLC is typically carried out by a device's designer and manufacturer, potentially with instructions or other input from the system's eventual operator. Such controls are considered below.

A. Use of all-source intelligence regarding component suppliers

The potential widespread use of advanced neuroprostheses by the public (including by the employees and customers of an organization's suppliers) may provide organizations with a new element to incorporate into all-source

[5] *NIST SP 800-53* (2013), p. F–110.

[6] See Chapter Three of this text for a discussion of the growing interconnection of information security with fields such as neuroscience and biomedical engineering, especially in the context of advanced neuroprosthetic devices.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

intelligence analysis: namely, the thoughts, memories, perceptions, plans, and emotions of individuals associated with current or potential suppliers that are publically shared by these persons through neuroprosthetically enabled social networks. This would represent a potentially deeper and more sophisticated source of information and analysis than can be obtained, for example, from the analysis of contemporary social media posts.[7]

B. Design of integrity indicators

1. Integrity checks for firmware and software

Checking the integrity of a device's operating system or applications[8] may be difficult or impossible in the case of some neuroprosthetic devices that utilize physical neural networks (and do not execute 'programs' as conventionally understood) or which are passive devices that are directly controlled by their host's cognitive processes, which effectively provide the 'operating system' for the device.[9] In the case of neuroprosthetic devices that utilize biological components for storing information and performing activities, it may be impossible to require the same level of integrity as that expected with electronic computers, insofar as the biological components may be undergoing gradual but continuous change through the birth, growth, mutation, and death of individual cells.

2. Tamper-detection mechanisms

Tamper-detection seals and anti-tamper coatings[10] may be utilized to prevent unauthorized access to a neuroprosthetic device's internal components or to ensure that if such components *have* been accessed by an unauthorized party, evidence of that unauthorized access will be visible to the next authorized party who conducts routine maintenance operations on or provides other service for the device.[11]

C. Designing the capacity to detect medical emergencies

A neuroprosthetically augmented information system may not only be able to detect errors and incidents relating to the electronic portion of the system but may also be able to directly or indirectly detect medical incidents

---

[7] Regarding all-source intelligence and component system suppliers, see *NIST SP 800-53* (2013), p. F–171.

[8] *NIST SP 800-53* (2013), p. F–225.

[9] See Chapter One of this text for a discussion of passive neuroprosthetic devices and Chapter Two for a discussion of integrity as an information security goal and attribute.

[10] *NIST SP 800-53* (2013), p. F–129.

[11] The systems described in Chapter Three of this text for providing audible – rather than visible – alerts to a device's host when attempts are made to wirelessly access the device constitute another kind of anti-tampering mechanism.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

and other biological problems affecting to the human host of an implanted neuroprosthesis. For example, Rasmussen et al. have proposed a model of emergency access control for implantable medical devices that relies on ultrasound technology to verify the physical proximity of an external system attempting to gain access to an IMD. Normally the IMD would require an external system to possess a shared cryptographic key before granting the external system access to the IMD; however if the IMD detects that its host is undergoing a medical emergency, it 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, as measured by the time required for ultrasound communications to travel between the IMD and external system.[12]

SDLC stage 3: device deployment in the host-device system and broader supersystem

The third stage in the system development life cycle includes the activities surrounding deployment of a neuroprosthesis in its human host (with whom it forms a biocybernetic host-device system) and the surrounding organizational environment or supersystem. The development or implementation of security controls in this stage of the SDLC is typically performed by a device's operator with the active or passive participation of its human host. Such controls are considered below.

A. Fostering of integrated situational awareness

Organizations integrate information obtained "from a combination of physical, cyber, and supply chain monitoring activities"[13] in order to better detect cyberattacks, which may be multifaceted operations that have both physical and virtual components and which target both an employer's operation of a neuroprosthesis and the suppliers who designed and produced the device's hardware and software components. For individual human hosts who operate neuroprostheses that they have purchased or leased as consumer electronics devices, developing such integrated situational awareness relating to their devices can be difficult. For such an individual, the physical monitoring of his or her device may be relatively easy, insofar as the device is always physically present with the host, and in order for unauthorized parties to physically access the device they may need to physically access or manipulate the host's biological body. Awareness of cyberattacks or other unauthorized

[12] 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.

[13] *NIST SP 800-53* (2013), p. F–222.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

electronic access may be more difficult for the host to achieve and may depend on a combination of effective security controls built into the device, its OS, and its applications, as well as personal knowledge of and commitment to InfoSec best practices on the part of the device's host. Full supply chain monitoring may be difficult or impossible for the host to carry out: although he or she may know the identity of the organizations that were responsible for assembling and distributing the finished physical device and its operating system and installed applications, it may be difficult for the host to determine who designed and manufactured individual components within the device or who may have served as a subcontractor writing and testing outsourced portions of the OS and applications on behalf of the primary developer. In the case of open-source software, it may be more difficult to know the true identity of the parties responsible for providing particular elements of code, although it may simultaneously be easier to scrutinize the content of the code itself.

B. Establishing baselines to detect atypical account usage

For some kinds of neuroprosthetic devices, it may be difficult to establish clear baselines and a definition of what constitutes 'typical' and 'atypical' usage,[14] just as it is difficult to clearly define what constitutes 'typical' thoughts, emotions, beliefs, volitions, or use of the imagination. This challenge may be exacerbated when a neuroprosthetic device is used to allow a user to interface with and experience some virtual environment that is, in a sense, already 'atypical' and likely to generate new kinds of activities and experiences.[15]

C. Activation of monitoring and scanning systems

1. Continuous monitoring, guards, and alarms

In the case of implantable neuroprosthetic devices, it may be possible to use one device as a 'guard' that monitors physical access to other devices implanted within the same human host.[16]

---

[14] *NIST SP 800-53* (2013), p. F–10.

[15] For some examples of neuroprosthetic devices that provide their hosts and users, e.g., with the sensorimotor experience of a new body that is (perhaps even radically) 'nonhuman,' see Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics: Video Games as Tools for Posthuman 'Body Schema (Re)Engineering'" (2015).

[16] Regarding continuous guards, alarms, and monitoring, see *NIST SP 800-53*, (2013), p. F–129. See the related discussion in Chapter Three of this text of proposed schemes for emergency access to IMDs that utilize external cloaking devices or gateway devices to mediate, limit, or control access to an implanted device.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

2. Specialized devices for information system monitoring

Significant legal, ethical, and practical questions arise regarding an organization's deployment of monitoring devices to observe and scrutinize an organizational information system.[17] Although such monitoring may have the legitimate purpose of detecting or dissuading attacks, it may sometimes also gather personal information on the activities, health, and other characteristics of organizational members or outside parties in ways that is legally and ethically impermissible. External systems (e.g., medical imaging or diagnostic equipment) may be used to monitor the activities of a neuroprosthetic device or host-device system; alternatively, a neuroprosthetic device may itself be used by an organization as a monitoring device to scrutinize the activity of other conventional information systems belonging to the organization (e.g., servers or desktop computers). Other implantable devices that are located within the same organism as a neuroprosthetic device may be used to monitor the activities of the device and its host-device system.[18]

3. Vulnerability scans

In some circumstances, even the mere act of scanning an implanted neuroprosthetic device to identify vulnerabilities[19] could be considered an invasive medical procedure and an infringement on the privacy of the human host in whom the device is implanted. In other circumstances, it might potentially be considered medical malpractice for an organization not to utilize all available means in probing neuroprosthetic devices implanted in its personnel to identify device vulnerabilities and the nature and extent of discoverable information within the devices and their connected systems that is potentially available to unauthorized parties.

4. Video surveillance

In the case of some neuroprosthetic devices such as artificial eyes, a device itself may be able to provide video surveillance[20] to its operator that records whether anyone has gained physical access to the device – with the caveat that if the device's security has already been compromised through some

[17] *NIST SP 800-53* (2013), pp. F–219-20.

[18] For a discussion of ethical and legal aspects relating to such issues, see Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); Mak, "Ethical Values for E-Society: Information, Security and Privacy" (2010); McGrath & Scanaill, "Regulations and Standards: Considerations for Sensor Technologies" (2013); Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010); and Brey, "Ethical Aspects of Information Security and Privacy" (2007).

[19] *NIST SP 800-53* (2013), p. F–153.

[20] *NIST SP 800-53* (2013), p. F–132.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

other means (e.g., if it has been hacked through use of software that had been installed on the device through a wireless connection), it may not be possible to trust the accuracy or integrity of any video stream being provided by the device, as that imagery could be fabricated or altered.[21]

An artificial eye may also be able to provide video surveillance that will allow its operators to determine whether any parties have acquired physical access to other neuroprosthetic devices implanted in the same host or, potentially, in other persons who are within the artificial eye's field of vision.

5. Systematic intrusion detection mechanisms

Intrusions *into* neuroprosthetic devices may be detected by standard tools that monitor the electronic components and systems of a device; they may also potentially be detected as alterations in a device's functioning by the human host with whose neural circuitry the device is integrated. Intrusions into conventional information systems committed *using* neuroprosthetic devices may – depending on the nature of the intrusion – be detected by traditional intrusion-detection mechanisms,[22] be detected by specialized detection mechanisms designed specifically to recognize the presence and activity of neuroprosthetic devices, or be difficult to detect by any means.[23]

6. Surveillance equipment for intrusion detection

Multiple neuroprosthetic devices may be able to create a body area network (BAN) or body sensory network (BSN) in which devices conduct mutual surveillance, monitor one another's status, and identify physical intrusions into their host's body or bodily systems.[24]

7. Technical surveillance countermeasures surveys

Technical surveillance countermeasures surveys are conducted in order "to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities."[25] They are generally performed using a combination of intensive electronic testing, visual observation, and physical

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

[22] Regarding system-wide intrusion detection systems, see *NIST SP 800-53* (2013), p. F–220.

[23] See Chapter Three of this text for a discussion of neuroprosthetic devices as potential tools for use in launching cyberattacks or other kinds of attacks.

[24] Regarding intrusion alarms and surveillance equipment, see *NIST SP 800-53* (2013), p. F–131.

[25] *NIST SP 800-53* (2013), p. F–155.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

examination of information systems, the facilities in which they are housed, and the surrounding environment.[26]

In the case of advanced neuroprostheses utilized by an organization, it may not always be legally, ethically, or practically feasible to conduct countermeasures surveys in all of the venues in which a neuroprosthetic device may operate (e.g., within the home of its human host), even with the advance consent of the host. Surveillance countermeasures surveys must also be conducted in a way that does not create a danger of physical or psychological harm for the host of a neuroprosthetic device or for others. Finally, it should be noted that in some cases the efficacy of surveillance countermeasures surveys that are planned and conducted in conjunction with the human host of a neuroprosthetic device may be compromised by the fact that one form of implementing a 'surveillance device' by adversaries would involve hacking a host's existing sensory organs, memory systems, or other cognitive processes in order to gain access to data gathered by or stored in a host's existing neuroprosthetic device.[27] In such a case, the adversary utilizing an existing neuroprosthesis as a surveillance device may – through the device – gain advance notice of planned surveillance countermeasures surveys and be able to evade them through appropriate planning. Moreover, some kinds of technical surveillance countermeasures surveys may be able to detect the presence of a surveillance device that should not have been present at all, but may have more difficulty detecting the fact that a human host's neuroprosthesis that was known to and whose presence was authorized by the organization had been hijacked or otherwise compromised by an adversary and was being (either temporarily, periodically, or permanently) employed by an unauthorized party as a surveillance device. It may be similarly difficult to detect situations in which an employee whose implanted neuroprosthesis is known to (and perhaps even provided by) his or her employer is being utilized by the employee in an unauthorized way as a surveillance device, particularly if the patterns of device activity reflected in such unauthorized uses are generally consistent with those seen when the device is used for authorized purposes.

8. Methods for detecting indicators of compromise

Organizations may use automated or manual procedures for searching for **indicators of compromise** (IOCs), which are detectable traces created or left within an information system that may indicate that the system has been compromised; such IOCs may include new registry key values or records of

[26] *NIST SP 800-53* (2013), p. F–155.

[27] See Chapter Three of this text for a discussion of the possibility of adversaries accessing another individual's neuroprosthetic device in order to create a surveillance instrument.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

network traffic between the system and known command-and-control servers.[28] In the case of advanced neuroprosthetic devices, IOCs may potentially take radically new and different forms, such as the presence of unexplained or corrupted memories or memory fragments within the mind of a device's host, the host's display of unusual sensory, motor, emotional, or personality-related behaviors, or the presence of particular hormones, other chemicals, or other objects within the host's bloodstream or body.[29]

SDLC stage 4: device operation within the host-device system and supersystem

The fourth stage in the system development life cycle involves the activities occurring after a neuroprosthetic device has been deployed in its production environment (comprising its host-device system and broader supersystem) and is undergoing continuous use in real-world operating conditions. The development or execution of security controls in this stage of the SDLC is typically carried out by a device's operator and maintenance service provider(s) with the active or passive participation of its human host. Such controls are considered below.

A. Ongoing general monitoring

1. Device monitoring and tracking

Monitoring and tracking the location[30] of an implanted neuroprosthetic device raises complex legal and ethical questions, insofar as this necessarily entails monitoring and tracking the location of the human host in whom it is implanted.

2. Incident monitoring

Conducting incident monitoring[31] to track and document security incidents may be difficult in the case of neuroprosthetic devices (such as those comprising biological components or nanorobotic swarms) that may lack a centralized mechanism capable of detecting and recording incidents affecting a device's components.[32]

---

[28] *NIST SP 800-53* (2013), p. F–223.

[29] For the possibility that an attack on a neuroprosthetic device or its host-device system might produce long-term changes in the neural activity or structures of the device's host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

[30] *NIST SP 800-53* (2013), p. F–138.

[31] *NIST SP 800-53* (2013), p. F–107.

[32] See the discussion of passive neuroprosthetic devices in Chapter One of this text for examples of such devices.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

3. Maintenance and scrutiny of visitor access records

It may be appropriate for the organization operating a neuroprosthetic device to record the identities and other details of individuals who gain direct physical access to the device itself; however, it may be legally or ethical questionable for the organization to record and archive details regarding the circumstances and identities of all individuals who gain physical access[33] to the device's host more generally (e.g., through face-to-face meetings or in other ways).

4. Collection and correlation of monitoring information

Given the resources needed for receiving, processing, and transmitting all of the monitoring data from a wide array of sources that is to be correlated,[34] such correlation may often be handled best by external systems that are managed by the operators of a neuroprosthetic device. The use of an external system that is housed within a conventional information systems facility avoids the severe limitations on memory storage, processing capacity, and communications bandwidth that affect many implantable neuroprosthetic devices due to their size, power, and operational constraints. Particular insights, conclusions, or instructions that result from the correlation of monitoring information in an external system can then be conveyed to a device or to its host or operator for use as appropriate.

C. Auditing of events

1. Specification of events to be audited

In the case of some neuroprostheses (such as those that utilize a physical neural network or are passive devices controlled by a host's neural circuitry[35]) it may be difficult to specify particular kinds of auditable events.[36]

2. Designing a storage system for audit data

Implantable neuroprosthetic devices may possess limited onboard capacity to store audit records generated by a device.[37] Offloading audit data to external systems for permanent storage may not be possible, for example, if a neuroprosthetic device includes a physical neural network with billions of neurons whose individual real-time actions have been designated as audit

[33] *NIST SP 800-53* (2013), p. F–132.

[34] *NIST SP 800-53* (2013), p. F–222.

[35] See the device ontology in Chapter One of Gladden, *Neuroprosthetic Supersystems Architecture* (2017), for a discussion of neuroprosthetic devices that utilize a physical neural network and Chapter One of this volume for a discussion of passive neuroprosthetic devices.

[36] *NIST SP 800-53* (2013), pp. F–41-42.

[37] Regarding audit storage capacity, see *NIST SP 800-53* (2013), p. F–43.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

events but which cannot be recorded and transmitted to external systems using current or foreseeable technologies.

3. Sensitivity of audit data

Monitoring the ways in which its operator or host utilizes a neuroprosthetic device raises legal and ethical questions insofar as such monitoring may capture and record personal medical data, the contents of cognitive processes, or other sensitive data about the status and actions of the device's human host.[38]

4. Protections for audit data

The use of hardware-enforced write-once media, cryptographic protection, read-only access, and data backup on separate physical systems is beneficial for ensuring information security for a device's audit information.[39] However, the use of such technologies and techniques may or may not be possible for a neuroprosthesis. For example, an implanted device may have no means of backing up audit data to external systems.[40]

5. Chain of custody of audit data (non-repudiation)

The chain of custody of audit information[41] may be difficult or impossible to maintain for a neuroprosthetic device that stores audit information within itself (without the possibility of backup to external systems) and which is not stored permanently within a single secured facility belonging to the operator but rather implanted in a human being who brings the device into environments and situations in which unauthorized attempts to access the device may easily be made.

D. Threat and incident detection

1. Inspection of devices and components after deployment

The inspection of a neuroprosthetic device after its implantation may require the express consent of the device's host.[42] There is a danger that if the

[38] Regarding such legal and ethical issues, see, e.g., Hildebrandt & Anrig, "Ethical Implications of ICT Implants" (2012); Kosta & Bowman (2012); McGrath & Scanaill (2013); and Shoniregun et al. (2010).

[39] *NIST SP 800-53* (2013), p. F–49.

[40] See Chapter Four of this text for the distinction between information stored by neuroprosthetic devices in the form of engrams versus exograms; information stored using exograms is typically easier to back up to external systems.

[41] *NIST SP 800-53* (2013), p. F–50.

[42] Regarding the inspection of information systems, devices, and components after their deployment, see *NIST SP 800-53* (2013), p. F–180.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

information security of an already-implanted device has indeed been compromised by an adversary – and the device is able to influence or exercise control over relevant biological or cognitive processes – then the human host may decline to express consent to an inspection not because the host has decided to reject the inspection through an act of his or her autonomous agency and volition but because the adversary has utilized control over the compromised device in a way that blocks the host from expressing agreement to an inspection.[43]

2. Security function verification during transitional states

In addition to regular ongoing security function verification, it is important to conduct special verification when a system is undergoing transitional states such as being powered on, rebooted, or shut down.[44] For some kinds of neuroprosthetic devices, key transitional states may also relate to the sensory, cognitive, and motor processes displayed by a device's human host, such as entering or leaving sleep, opening or closing eyelids, or initiating gross motor movements.

3. Non-signature-based detection of malicious code

Heuristic analysis and other approaches or mechanisms can be used to identify malicious code that is polymorphic or metamorphic and which cannot be identified by antivirus software that searches for particular known signatures.[45] In the case of some kinds of neuroprosthetic devices (e.g., those that utilize certain types of physical neural networks and do not execute programs as traditionally understood), malicious 'code' may not take the form of discrete strings of digital information that can be analyzed to detect particular signatures but may instead take the form of sense data or other forms of environmental phenomena that can affect a neuroprosthetic device or host-device system. In such situations, the use of heuristic analysis and probabilistic methods to identify potentially malicious input may be necessary.[46]

---

[43] See Chapter Three of this text for the related possibility of a neuroprosthetic device that unintentionally traps the mind of its human host within a 'zombie-like' host-device system in which the host is unable to express his or her thoughts or volitions using motor activity.

[44] *NIST SP 800-53* (2013), pp. F–224-25.

[45] *NIST SP 800-53* (2013), p. F–218.

[46] For some such neuroprosthetic systems, the process of detecting a malicious vector may be less like the discrete process of detecting a traditional computer virus (e.g., a kind of binary data file) and more like the ambiguous everyday challenge of identifying a potentially malicious *person*, a potentially damaging social relationship, or a potentially harmful sensory experience.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

4. Analysis of malicious code to ascertain effects

In the case of neuroprosthetic devices that utilize biological components or materials, 'malicious code' may potentially take the form of genetic sequences delivered through the use of biological (and not computer) viruses, microorganisms, or other biological vectors.[47] A sophisticated attack on such a neuroprosthetic device might combine both the use of a computer virus or worm that infects and compromises electronic portions of the device and a biological vector that infects and compromises the biological portions of the device. In the case of a neuroprosthesis that controls, supports, or executes the production of hormones, cells, or other biochemical products within its host's body, a computer worm or virus or attack that compromises the electronic portion of the device could conceivably be used to generate biochemical agents that would in turn infect and compromise biological components of the neuroprosthetic device or of the host's natural organism. Conversely, a biological vector or biochemical agent that infects biological components of the host's organism or of a neuroprosthetic device could conceivably be used to introduce malware into the device's electronic components, if the device's electronic components receive and process information or other input from biological or biochemical components or systems within the host's organism or the neuroprosthetic device.

5. Detection of unauthorized commands

Information systems are often designed to detect unauthorized operating system commands at the level of the kernel application programming interface, block the execution of such commands, and issue an alert.[48] Such mechanisms are important not just for preventing certain kinds of attacks that are purposefully launched against information systems by adversaries but also for preventing unauthorized commands that may be an unintentional result of some hardware or software failure, quantum-level metastability, or other phenomenon. Guarding against the execution of unauthorized commands is especially important in the case of neuroprosthetic devices with critical health impacts for their human host.

6. Detection of communication or possession of unsanctioned information

Controls may be used, for example, to detect proprietary or classified information whose possession would be unlawful and to block it from being transferred into a host's memory by his or her neuroprosthetic device.[49]

---

[47] Regarding malicious code analysis, see *NIST SP 800-53* (2013), p. F–219.

[48] *NIST SP 800-53* (2013), p. F–218.

[49] For controls relating to unsanctioned information, see *NIST SP 800-53* (2013), p. F–17.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

7. Identification and analysis of covert channels

An organization typically identifies ways in which devices or systems emit transmissions, material objects, or other phenomena that could be used as covert channels for communication; determines the maximum bandwidth available through such covert channels for potential unauthorized communications; and attempts to reduce the bandwidth available for covert channels, insofar as this is feasible given the organization's functional needs and operational priorities.[50] Some kinds of neuroprosthetic devices may not only generate phenomena such as wireless transmissions, magnetic fields, electrical charges, heat, biological or biochemical substances and materials, and other objects or phenomena that can be directly observed by external parties; the devices may also stimulate the body of their human host in a way that causes it to produce physical reactions or behaviors that can be observed by persons or sensors in the external environment and which can potentially serve as covert channels for the communication of information. It may not be legally, ethically, or practically possible to eliminate or minimize the bandwidth of all such channels.

8. Detection of anomalous communications traffic

In the case of general-purpose organizational information systems, anomalous communications traffic may include "large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses."[51]

In the case of neuroprosthetic devices, anomalous traffic at the external boundaries of a device may result from unusually intense or numerous environmental stimuli impacting a sensory neuroprosthetic (perhaps reaching the level of sensory overload), unusually intense or complex motor instructions being sent to motor organs (e.g., when attempting to speak, play a musical instrument, or engage in sports activities), or unusually intense, rich, or complex cognitive activities (e.g., caused by or reflected in heightened emotion, a state of dreaming or hallucination, acts of mental calculation, the imagining of new ideas, or the retrieval of distant memories). Note that activities seen as producing 'anomalous' communications traffic patterns when viewed in relation to a neuroprosthetic device may appear quite commonplace from the perspective of the device's human host.

[50] *NIST SP 800-53* (2013), pp. F–206-07.

[51] *NIST SP 800-53* (2013), p. F–221.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

9. Detection of wireless intrusions

Organizations may use a wireless intrusion detection system to scan for and detect both the connection of unauthorized wireless devices to the organization's own wireless access points as well as the presence of unauthorized wireless access points within organizational facilities.[52] Such wireless intrusion detection systems may be used, for example, to identify visitors to organizational facilities who are using nonvisible neuroprosthetic devices to make unauthorized connections to organizational information systems or to identify miniaturized neuroprosthetic devices that may have been implanted in organizational personnel without their knowledge and which are attempting to wirelessly contact command-and-control servers for instructions or to transmit gathered intelligence.[53]

10. Detection of extrusion and exfiltration attempts

The analysis of traffic to detect and prevent covert exfiltration[54] may be desirable and necessary even in the case of neuroprosthetic devices whose actions are clearly visible to their human host and which are theoretically engineered to transmit information or perform actions only in accordance with the volition of their host. For example, an advanced neuroprosthetic arm may be controlled by motor impulses originating in its host's brain, and its movements are visible to the eyes of its human host. However, a computer virus or adversary's cyberattack that is able to compromise the device and alter the motor instructions received by the device from its host's brain (or fabricate nonexistent motor instructions) may be able to cause the neuroprosthetic arm to move in minute ways or with subtly altered patterns that are undetectable to the host's natural biological eyes and visual perception but which can be detected and interpreted by external adversarial systems and used to exfiltrate information from the device or its host-device system.[55] In a sense, such a case would represent a form of **cognitive steganography** or **motor steganography**.

---

[52] *NIST SP 800-53* (2013), p. F–222.

[53] See Chapter Three of this text for a discussion of the reliance on wireless communication demonstrated by many kinds of neuroprosthetic devices.

[54] *NIST SP 800-53* (2013), p. F–222.

[55] Regarding the possibility that a neuroprosthetic limb could be hacked or otherwise compromised by an adversary and that its behavior could be remotely controlled or manipulated, see Denning et al. (2009).

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

E. Proactive detection and analysis methods

1. Use of devices as active honeyclients

It is theoretically possible to use neuroprosthetic devices (or their constituent components, subsystems, or subnetworks) as honeyclients[56] that proactively explore the Internet in search of malicious code – either code designed to infect and harm a device itself or (e.g., if the neuroprosthetic device is being used by cyberwarfare personnel within a military organization) designed to infect other kinds of systems that the operator of the neuroprosthetic device has an interest in protecting. However, the legal and ethical implications of such practices must be carefully considered, especially if they create an increased risk that the human host or operator of a neuroprosthetic device may experience physical or psychological damage as a result of the device's intentional encounter with malicious code.

2. Use of devices as passive honeypots

It may or may not be feasible to provide a neuroprosthetic device itself with the components, subsystems, or subnetworks needed to create a honeypot[57] that can either simply serve as a decoy that lures the attention of adversaries away from the device's actual core systems or which potentially allows adversaries' attacks to be observed and analyzed without creating a danger for the device's core systems. In many cases, it may not be an effective use of the limited resources that can be included in a small implantable device to create a honeypot within the device itself. Unique legal and ethical issues (including those of liability for possible damages to the host) may also arise through creating within the body of a human host such decoy systems that can attract attacks.

In some cases (e.g., those of neuroprosthetic devices that are composed largely or entirely of biological material, do not have significant mechanisms for communicating with the environment external to their human host, and are not easily detectable using the sort of electronic equipment that is typically used to detect and analyze mobile computers), it may be more prudent, effective, and efficient to attempt to entirely mask and conceal the device's existence than to create a honeypot which, in a sense, is purposefully designed to attract attention.[58]

[56] *NIST SP 800-53* (2013), p. F–208.

[57] *NIST SP 800-53* (2013), p. F–202.

[58] See Chapter Three of this text for proposed approaches that utilize shielding or jamming in an attempt to conceal the existence of a neuroprosthetic device.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

SDLC stage 5: device disconnection, removal, and disposal

The fifth stage in the system development life cycle involves a neuroprosthetic device's functional removal from its host-device system and broader supersystem; this may be accomplished through means such as remote disabling of the device or its core functionality, surgical extraction of the device, or the device's physical disassembly or destruction. The stage also includes a device's preparation for reuse or ultimate disposal after removal from its previous human host. The development or execution of security controls in this stage of the SDLC is typically performed by a device's operator or maintenance service provider(s), potentially with the active or passive participation of its human host. In this text, we do not identify any standard detective InfoSec controls as finding their greatest possible relevance during this final stage of the SDLC.

Conclusion

In this chapter, we have reviewed a number of detective security controls for information systems and discussed the implications of applying such controls to neuroprosthetic devices and the larger information systems in which they participate, using the lens of a five-stage system development life cycle as a conceptual framework. In the following chapter, a similar analysis of corrective and compensating controls will be undertaken.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

References

Abrams, Jerold J. "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault." *Human Studies* 27, no. 3 (2004): 241-58.

Al-Hudhud, Ghada. "On Swarming Medical Nanorobots." *International Journal of Bio-Science & Bio-Technology* 4, no. 1 (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 (2010): 93-101.

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.

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, pp. 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* (2014): 1-18.

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, pp. 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.

Baddeley, Alan. "The episodic buffer: a new component of working memory?" *Trends in cognitive sciences* 4, no. 11 (2000): 417-23.

Badmington, Neil. "Cultural Studies and the Posthumanities," edited by Gary Hall and Claire Birchall. *New Cultural Studies: Adventures in Theory*, pp. 260-72. Edinburgh: Edinburgh University Press, 2006.

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

Bendle, Mervyn F. "Teleportation, cyborgs and the posthuman ideology." *Social Semiotics* 12, no. 1 (2002): 45-62.

Benedict, M., and H. Schlieter. "Governance Guidelines for Digital Healthcare Ecosystems," in *EHealth2015 – Health Informatics Meets EHealth: Innovative Health Perspectives: Personalized Health,* pp. 233-40. 2015.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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, pp. 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 Alfons J. Schuster, pp. 129-52. Springer London, 2007.

Birnbacher, Dieter. "Posthumanity, Transhumanism and Human Nature." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, pp. 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, pp. 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, pp. 107-36. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Bostrom, Nick, and Anders Sandberg. "Cognitive Enhancement: Methods, Ethics, Regulatory Challenges." *Science and Engineering Ethics* 15, no. 3 (2009): 311-41.

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, pp. 175-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

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, pp. 21-36. Data-Centric Systems and Applications. Springer Berlin Heidelberg, 2007.

"Bridging the Bio-Electronic Divide." Defense Advanced Research Projects Agency, January 19, 2016. http://www.darpa.mil/news-events/2015-01-19. Accessed May 6, 2016.

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, pp. 719-23. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Buller, Tom. "Neurotechnology, Invasiveness and the Extended Mind." *Neuroethics* 6, no. 3 (2011): 593-605.

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, pp. 199-257. Philosophy and Medicine 98. Springer Netherlands, 2008.

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, pp. 437-42. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Chadwick, Ruth. "Therapy, Enhancement and Improvement." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, pp. 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 and Sohail Chaudhry, pp. 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, pp. 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, 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, pp. 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 (2012): 211-14.

Clowes, Robert W. "The Cognitive Integration of E-Memory." *Review of Philosophy and Psychology* 4, no. 1 (2013): 107-33.

Coeckelbergh, Mark. "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, pp. 45-71. Advances in Information Security 49. Springer US, 2010.

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: US Food and Drug Administration, 2014.

Cosgrove, G.R. "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.

"Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication." U.S. Food and Drug Administration, June 13, 2013. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm. Accessed May 3, 2016.

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

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*, pp. 184-93. IEEE, 2004.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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*, pp. 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.

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, pp. 724-31. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Dormer, Kenneth J. "Implantable electronic otologic devices for hearing rehabilitation." In *Handbook of Neuroprosthetic Methods*, edited by Warren E. Finn and Peter G. LoPresti, pp. 237-60. Boca Raton: CRC Press, 2003.

Drongelen, Wim van, Hyong C. Lee, and Kurt E. Hecox. "Seizure Prediction in Epilepsy." In *Neural Engineering*, edited by Bin He, pp. 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.

Durand, Dominique M., Warren M. Grill, and Robert Kirsch. "Electrical Stimulation of the Neuromuscular System." In *Neural Engineering*, edited by Bin He, pp. 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.

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, pp. 1003-17. Springer Berlin Heidelberg, 2011.

Erler, Alexandre. "Does Memory Modification Threaten Our Authenticity?" *Neuroethics* 4, no. 3 (2011): 235-49.

Evans, Dave. "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World." Cisco Internet Solutions Business Group: Point of View, 2012. https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf. Accessed December 16, 2015.

Fairclough, S.H. "Physiological Computing: Interfacing with the Human Nervous System." In *Sensing Emotions*, edited by J. Westerink, M. Krans, and M. Ouwerkerk, pp. 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 (2013): 113-70.

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.

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: National Institute of Standards and Technology, 2004.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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.

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, pp. 357-62. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

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*, pp. 82-85. IEEE, 2007.

Friedenberg, Jay. *Artificial Psychology: The Quest for What It Means to Be Human*. Philadelphia: Psychology Press, 2008.

Fukuyama, Francis. *Our Posthuman Future: Consequences of the Biotechnology Revolution*. New York: Farrar, Straus, and Giroux, 2002.

Gärtner, Armin. "Communicating Medical Systems and Networks." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, pp. 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, pp. 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, pp. 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, pp. 287-95. Springer US, 2008.

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

Gladden, Matthew E. "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values." *Annales: Ethics in Economic Life* vol. 18, no. 4 (2015): 85-98.

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

Gladden, Matthew E. "The Diffuse Intelligent Other: An Ontology of Nonlocalizable Robots as Moral and Legal Actors." In *Social Robots: Boundaries, Potential, Challenges*, edited by Marco Nørskov, pp. 177-98. Farnham: Ashgate, 2016.

Gladden, Matthew E. "Enterprise Architecture for Neurocybernetically Augmented Organizational Systems: The Impact of Posthuman Neuroprosthetics on the Creation of Strategic, Structural, Functional, Technological, and Sociocultural Alignment." Thesis project, MBA in Innovation and Data Analysis. Warsaw: Institute of Computer Science, Polish Academy of Sciences, 2016.

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, pp. 219-26. Annals of Computer Science and Information Systems 3. Polskie Towarzystwo Informatyczne, 2014.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Gladden, Matthew E. *The Handbook of Information Security for Advanced Neuroprosthetics.* Indianapolis: Synthypnion Academic, 2015.

Gladden, Matthew E. "Information Security Concerns as a Catalyst for the Development of Implantable Cognitive Neuroprostheses." In *9th Annual EuroMed Academy of Business (EMAB) Conference: Innovation, Entrepreneurship and Digital Ecosystems (EUROMED 2016) Book of Proceedings*, edited by Demetris Vrontis, Yaakov Weber, and Evangelos Tsoukatos, pp. 891-904. Engomi: EuroMed Press, 2016.

Gladden, Matthew E. "Managing the Ethical Dimensions of Brain-Computer Interfaces in eHealth: An SDLC-based Approach." In *9th Annual EuroMed Academy of Business (EMAB) Conference: Innovation, Entrepreneurship and Digital Ecosystems (EUROMED 2016) Book of Proceedings*, edited by Demetris Vrontis, Yaakov Weber, and Evangelos Tsoukatos, pp. 876-90. Engomi: EuroMed Press, 2016.

Gladden, Matthew E. "Neural Implants as Gateways to Digital-Physical Ecosystems and Posthuman Socioeconomic Interaction." In *Digital Ecosystems: Society in the Digital Age*, edited by Łukasz Jonak, Natalia Juchniewicz, and Renata Włoch, pp. 85-98. Warsaw: Digital Economy Lab, University of Warsaw, 2016.

Gladden, Matthew E. *Neuroprosthetic Supersystems Architecture.* Indianapolis: Synthypnion Academic, 2017.

Gladden, Matthew E. *Sapient Circuits and Digitalized Flesh: The Organization as Locus of Technological Posthumanization*. Indianapolis: Defragmenter Media, 2016.

Gladden, Matthew E. "Utopias and Dystopias as Cybernetic Information Systems: Envisioning the Posthuman Neuropolity." *Creatio Fantastica* nr 3 (50) (2015).

Graham, Elaine. *Representations of the Post/Human: Monsters, Aliens and Others in Popular Culture*. Manchester: Manchester University Press, 2002.

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*, pp. 187-206. Lecture Notes in Computer Science 5017. Springer Berlin Heidelberg, 2008.

Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. Silver Spring, MD: US Food and Drug Administration, 2005.

Gunkel, David J. *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*. Cambridge, MA: The MIT Press, 2012.

Gunther, N. J. "Time—the zeroth performance metric." In *Analyzing Computer System Performance with Perl::PDQ*, 3-46. Berlin: Springer, 2005.

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.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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*, pp. 13-20. ACM, 2010.

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

Haraway, Donna. "A Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s." *Socialist Review* 15, no. 2 (1985): 65-107.

Haraway, Donna. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge, 1991.

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, pp. 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, pp. 810-17. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Hayles, N. Katherine. *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press, 1999.

Heersmink, Richard. "Embodied Tools, Cognitive Tools and Brain-Computer Interfaces." *Neuroethics* 6, no. 1 (2011): 207-19.

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

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

Herbrechter, Stefan. *Posthumanism: A Critical Analysis*. London: Bloomsbury, 2013. [Kindle edition.]

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.

Heylighen, Francis. "The Global Brain as a New Utopia." In *Renaissance der Utopie. Zukunftsfiguren des 21. Jahrhunderts*, edited by R. Maresch and F. Rötzer. Frankfurt: Suhrkamp, 2002.

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, pp. 135-58. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Hochmair, Ingeborg. "Cochlear Implants: Facts." MED-EL, September 2013. http://www.medel.com/cochlear-implants-facts. Accessed December 8, 2016.

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, pp. 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, pp. 266-73. Lecture Notes in Computer Science 6686. Springer Berlin Heidelberg, 2011.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

IEC 80001: Application of risk management for IT-networks incorporating medical devices, Parts 1 through 2-7. ISO/TC 215. Geneva: IEC, 2010-15.

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

ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002. ISO/TC 215. Geneva: ISO/IEC, 2008.

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC JTC 1/SC 27. Geneva: ISO/IEC, 2013.

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls. ISO/IEC JTC 1/SC 27. Geneva: ISO/IEC, 2013.

ISO/TR 11633-1:2009, Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis. ISO/TC 215. Geneva: ISO, 2009.

ISO/TR 11633-2:2009, Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 2: Implementation of an information security management system (ISMS). ISO/TC 215. Geneva: ISO, 2009.

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

Kelly, Kevin. "A Taxonomy of Minds." *The Technium*, February 15, 2007. http://kk.org/thetechnium/a-taxonomy-of-m/. Accessed January 25, 2016.

Kelly, Kevin. "The Landscape of Possible Intelligences." *The Technium*, September 10, 2008. http://kk.org/thetechnium/the-landscape-0/. Accessed January 25, 2016.

Kelly, Kevin. *Out of Control: The New Biology of Machines, Social Systems and the Economic World*. Basic Books, 1994.

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.

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, pp. 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, pp. 241-67. The Frontiers Collection. Springer Berlin Heidelberg, 2012.

Koops, B.-J., and R. Leenes. "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes." In *Human ICT Implants: Technical, Legal and Ethical*

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Considerations, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, pp. 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, pp. 97-112. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Kourany, J.A. "Human Enhancement: Making the Debate More Productive." *Erkenntnis* 79, no. 5 (2013): 981-98.

Kowalewska, Agata. "Symbionts and Parasites – Digital Ecosystems." In *Digital Ecosystems: Society in the Digital Age*, edited by Łukasz Jonak, Natalia Juchniewicz, and Renata Włoch, pp. 73-84. Warsaw: Digital Economy Lab, University of Warsaw, 2016.

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

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 (2014): 99-110.

Leder, Felix, Tillmann Werner, and Peter Martini. "Proactive Botnet Countermeasures: An Offensive Approach." In *The Virtual Battlefield: Perspectives on Cyber Warfare,* volume 3, edited by Christian Czosseck and Kenneth Geers, pp. 211-25. IOS Press, 2009.

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 (2014): 1-23.

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

Lind, Jürgen. "Issues in agent-oriented software engineering." In *Agent-Oriented Software Engineering*, pp. 45-58. Springer Berlin Heidelberg, 2001.

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

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

Lucivero, Federica, and Guglielmo Tamburrini. "Ethical Monitoring of Brain-Machine Interfaces." *AI & SOCIETY* 22, no. 3 (2007): 449-60.

Ma, Ting, Ying-Ying Gu, and Yuan-Ting Zhang. "Circuit Models for Neural Information Processing." In *Neural Engineering*, edited by Bin He, pp. 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.

Maguire, Gerald Q., and Ellen M. McGee. "Implantable brain chips? Time for debate." *Hastings Center Report* 29, no. 1 (1999): 7-13.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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 Research Centre / 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, pp. 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, pp. 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, pp. 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 (2013): 109-22.

McGee, E.M. "Bioelectronics and Implanted Devices." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, pp. 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*, pp. 115-35. Apress, 2013.

McIntosh, Daniel. "The Transhuman Security Dilemma." *Journal of Evolution and Technology* 21, no. 2 (2010): 32-48.

Medical Enhancement and Posthumanity, edited by Bert Gordijn and Ruth Chadwick. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Meloy, Stuart. "Neurally Augmented Sexual Function." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, pp. 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*, pp. 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, pp. 71-94. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

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, pp. 241-58. The Frontiers Collection. Springer Berlin Heidelberg, 2009.

Miller, Jr., Gerald Alva. "Conclusion: Beyond the Human: Ontogenesis, Technology, and the Posthuman in Kubrick and Clarke's 2001." In *Exploring the Limits of the Human through Science Fiction*, pp. 163-90. American Literature Readings in the 21st Century. Palgrave Macmillan US, 2012.

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,* pp. 3432-36. IEEE, 2010.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Mizraji, Eduardo, Andrés Pomi, and Juan C. Valle-Lisboa. "Dynamic Searching in the Brain." *Cognitive Neurodynamics* 3, no. 4 (2009): 401-14.

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, pp. 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, pp. 209-14. IFMBE Proceedings 26. 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 800-100: Information Security Handbook: A Guide for Managers. Edited by P. Bowen, J. Hash, and M. Wilson. Gaithersburg, Maryland: National Institute of Standards & Technology, 2006.

NIST Special Publication 1800-1: Securing Electronic Health Records on Mobile Devices (Draft), Parts a, b, c, d, and e. Edited by G. O'Brien, N. Lesser, B. Pleasant, S. Wang, K. Zheng, C. Bowers, K. Kamke, and L. Kauffman. Gaithersburg, Maryland: National Institute of Standards & Technology, 2015.

Ochsner, Beate, Markus Spöhrer, and Robert Stock. "Human, non-human, and beyond: cochlear implants in socio-technological environments." *NanoEthics* 9, no. 3 (2015): 237-50.

Overman, Stephenie. "Jamming Employee Phones Illegal." Society for Human Resource Management, May 9, 2014. http://www.shrm.org/hrdisciplines/technology/articles/pages/cellphone-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, pp. 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, pp. 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*, fourth edition, 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.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Patil, P.G., and D.A. Turner. "The Development of Brain-Machine Interface Neuroprosthetic Devices." *Neurotherapeutics* 5, no. 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, pp. 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.

Posthuman Bodies, edited by Judith Halberstam and Ira Livingstone. Bloomington, IN: Indiana University Press, 1995.

Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: US Food and Drug Administration, 2016.

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 (1999): 205-14.

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

Principe, José C., and Dennis J. McFarland. "BMI/BCI Modeling and Signal Processing." In *Brain-Computer Interfaces*, pp. 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, pp. 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, Umesh Hodeghatta, and Umesha Nayak. *The InfoSec Handbook*. New York: Apress, 2014.

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).

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*, pp. 410-19. ACM, 2009.

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, pp. 166-70. National Science Foundation, 2002.

Roden, David. *Posthuman Life: Philosophy at the Edge of the Human*. Abingdon: Routledge, 2014.

Roosendaal, Arnold. "Carrying Implants and Carrying Risks; Human ICT Implants and Liability." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

N. Gasson, Eleni Kosta, and Diana M. Bowman, pp. 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, pp. 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*, pp. 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, pp. 55-62. 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, pp. 63-66. 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, pp. 29-39. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rowlands, Mark. *Can Animals Be Moral?* Oxford: Oxford University Press, 2012.

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

Rutherford, Andrew, Gerasimos Markopoulos, Davide Bruno, and Mirjam Brady-Van den Bos. "Long-Term Memory: Encoding to Retrieval." In *Cognitive Psychology*, second edition, edited by Nick Braisby and Angus Gellatly, pp. 229-65. Oxford: Oxford University Press, 2012.

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 Brian A. Simpson, pp. 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, pp. 3-13. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Sandberg, Anders. "Ethics of brain emulations." *Journal of Experimental & Theoretical Artificial Intelligence* 26, no. 3 (2014): 439-57.

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): 122-31.

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 (2009): 217-30.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

"Security Risk Assessment Framework for Medical Devices." Washington, DC: Medical Device Privacy Consortium, 2014.

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

Soussou, Walid V., and Theodore W. Berger. "Cognitive and Emotional Neuroprostheses." In *Brain-Computer Interfaces*, pp. 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, pp. 101-17. Arlington, Virginia: National Science Foundation, 2002.

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, pp. 435-42. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Szoldra, P. "The government's top scientists have a plan to make military cyborgs." Tech Insider, January 22, 2016. http://www.techinsider.io/darpa-neural-interface-2016-1. Accessed May 6, 2016.

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, pp. 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, pp. 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 (2009): 137-49.

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

Thanos, Solon, P. Heiduschka, and T. Stupp. "Implantable Visual Prostheses." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, pp. 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, pp. 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*, pp. 45-56. ACM, 2005.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Troyk, Philip R., and Stuart F. Cogan. "Sensory Neural Prostheses." In *Neural Engineering*, edited by Bin He, pp. 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, pp. 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.*

Van den Berg, Bibi. "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, pp. 159-73. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

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, pp. 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, pp. 481-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Wager, K.A., F. Wickham Lee, and J.P. Glaser. *Health Care Information Systems: A Practical Approach for Health Care Management.* John Wiley & Sons, 2013.

Wallach, Wendell, and Colin Allen. *Moral machines: Teaching robots right from wrong.* Oxford University Press, 2008.

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

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

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

Weinberger, Sharon. "Mind Games." *Washington Post*, January 14, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399.html. Accessed July 26, 2015.

"Welcome." Medical Device Privacy Consortium. http://deviceprivacy.org. Accessed May 6, 2016.

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

Westlake, Philip R. "The possibilities of neural holographic processes within the brain." *Biological Cybernetics* 7, no. 4 (1970): 129-53.

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, pp. 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, MA: The MIT Press, 1961. [Quid Pro ebook edition for Kindle, 2015.]

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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): 428-33.

Wooldridge, M., and N. R. Jennings. "Intelligent agents: Theory and practice." *The Knowledge Engineering Review*, 10(2) (1995): 115-52.

Yampolskiy, Roman V. "The Universe of Minds." arXiv preprint, *arXiv:1410.0369 [cs.AI]*, October 1, 2014. http://arxiv.org/abs/1410.0369. Accessed January 25, 2016.

Yonck, Richard. "Toward a standard metric of machine intelligence." *World Future Review* 4, no. 2 (2012): 61-70.

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.

Zaród, 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).

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 (2009): 78-87.

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)*, pp. 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)*, pp. 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)*, pp. 624-28. IEEE, 2014.

"Detective Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Seven in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 248-65.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).