Chapter Eight

Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems

Abstract. This chapter explores the way in which standard corrective and compensating 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.

Corrective and compensating controls considered include those relating to incident response procedures, mechanisms, and training; error handling capacities; failure mode capacities and procedures; and flaw remediation.

Introduction

In this chapter, we review a range of standard corrective and compensating security controls for information systems and identify unique issues 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 elements. The text applies such security controls without providing a detailed explanation of their workings; 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).

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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 InfoSec researchers categorize 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 classified controls as either **management**, **operational**, or **technical** controls. 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 incorporate 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 two chapters discussed the first two types of controls, while this chapter investigates the final type.

Role of security controls in the system development life cycle

The corrective and compensating controls discussed in this chapter 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 another stage. Here we attempt to locate a control in the SDLC stage in which decisions or actions are undertaken that have the greatest impact on the success

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

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

[4] A four-stage SDLC for health care information systems is described in Wager et al., *Health Care Information Systems: A Practical Approach for Health Care Management* (2013), a four-stage SDLC for an open eHealth ecosystem in Benedict & Schlieter, "Governance Guidelines for Digital Healthcare Ecosystems" (2015), pp. 236-37, and a generalized five-stage SDLC for information systems in *Governance Guidelines for Digital Healthcare Ecosystems* (2006), pp. 19-25. These are synthesized to create a five-stage SDLC for information systems incorporating brain-computer interfaces in Gladden, "Managing the Ethical Dimensions of Brain-Computer Interfaces in eHealth: An SDLC-based Approach" (2016).

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

or failure of the given control. This stage-by-stage discussion of corrective and compensating controls begins below.

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. Such controls are considered below.

A. Developing incident response procedures

1. Incident response teams

The use of dedicated organizational incident response teams[5] or services that proactively respond to an ongoing incident (e.g., by physically locating the host of a neuroprosthetic device, assessing his or her condition, and providing containment and recovery services) may be especially necessary in the case of a neuroprosthesis whose anomalous functioning may render its host incapacitated and unable to respond to an incident himself or herself.

2. Incident reporting methods

Various incident reporting[6] complications can arise with neuroprosthetically augmented information systems. For example, in the case of a human host who does not even realize that he or she has been implanted with a neuroprosthetic device, the host might discern that he or she is undergoing some unusual experience but would not associate it with the device and may have no ability to report the incident to the device's operator.[7]

3. Design of fail-safe procedures for the supersystem

The design and implementation of effective fail-safe procedures[8] is essential for ensuring information security for advanced neuroprosthetic devices and host-device systems, especially those with critical health impacts for a

[5] *NIST SP 800-53* (2013), p. F–108.

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

[7] For the possibility that human hosts might unwittingly be implanted, e.g., with certain kinds of RFID devices, see Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[8] *NIST SP 800-53* (2013), p. F–233.

device's host. Such procedures may require, for example, that the host or operator of a neuroprosthetic device receive a clear automated alert upon the failure or impending failure of critical device components, systems, or processes, along with explicit instructions of steps that should be taken. In the event of some failures by certain kinds of neuroprosthetic devices, a device's host may have only minutes or seconds in which to execute specified fail-safe procedures before the failure incapacitates the host or otherwise renders him or her unable to take additional action. Other specific fail-safe procedures may include enabling mechanisms that will allow emergency medical personnel to access a neuroprosthetic device, initiating the backup of key information maintained in volatile memory, or releasing particular biochemical agents to stimulate a specific response in the body of the device's host.[9]

B. Planning of incident response training

1. Designing incident response training

Incident response training[10] is especially important for the human host of an advanced neuroprosthesis, insofar as an incident relating to such a device does not compromise or damage some external system like a desktop computer or smartphone but may actually compromise the host's own biological and cognitive processes. Once an incident is underway, a device's host may only have a very limited time in which to react and carry out response measures before losing consciousness or losing control over his or her own volition, memory, or other mental processes. Specialized incident response training can help ensure that a device's host recognizes and responds to an ongoing incident in a timely and effective manner.

2. Planning of automated training environments

An organization or individual may utilize "automated mechanisms to provide a more thorough and realistic incident response training environment."[11] With some kinds of neuroprosthetic devices, automated training environments that are governed by artificially intelligent systems may be needed to accurately simulate or replicate the activity of adversaries whose capacities and techniques exceed the limits of what can be possessed or performed by an unaugmented human adversary.

[9] See Chapter Three of this text for a discussion of failure modes for neuroprosthetic devices and the need to provide adequate access to emergency medical personnel when a device's host is experiencing a medical emergency.

[10] *NIST SP 800-53* (2013), p. F–103.

[11] *NIST SP 800-53* (2013), p. F–104.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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 performed 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. Error handling capacities

1. Design of error handling procedures

Error messages generated by information systems should generally provide the kinds of information needed for organizational personnel to identify and remedy the source of the error without providing information that could be used by adversaries to either directly compromise a system or indirectly learn more about its functioning.[12] In the case of neuroprosthetic devices with critical health impacts, error messages may need to be presented not only through internal sensory or cognitive processes to a device's host or through organizational information systems to the device's operator but potentially also to emergency medical personnel who previously had no connection to the host or the host's organization but who happened to be in the vicinity of a host, are diagnosing and treating him or her for some health emergency, and may not (yet) have full access to the neuroprosthetic device's components or processes.[13]

2. Designing automated responses to integrity violations

Care must be taken that any automated responses to integrity violations[14] detected within a neuroprosthetic device do not cause physical or psychological harm to the device's host or others. In some circumstances, automated responses may need to be delayed in order to prevent a device from malfunctioning or failing when it is being used by its host or operator to perform an

[12] *NIST SP 800-53* (2013), p. F–230.

[13] Chapter Three of this text considers many proposed technological approaches for granting emergency medical personnel access to a neuroprosthetic device in cases when its human host is experiencing a medical emergency. An underappreciated aspect of such situations is the fact that even if emergency medical personnel have the technological means by which to gain access to a particular neuroprosthetic device, this in no way guarantees that they will have the expertise in computer science, information technology, biomedical engineering, or cybernetics that may be required in order to quickly diagnose the device's status and functioning, alter its configuration, and perhaps even reprogram it in order to yield specific positive outcomes for and impacts on the host's biological organism.

[14] *NIST SP 800-53* (2013), p. F–226.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

urgent task (e.g., with potentially critical health impacts for the device's host). In other circumstances, an automated response may *need* to take place instantaneously in order to protect the device's host or operator from some critical health impact.

3. Integration of incident detection and response

In the case of certain neuroprostheses – for example, some utilizing a physical neural network that is broadly interconnected with the neural circuitry of the brain of the devices' host and whose operating system or applications are partly or wholly stored within the biological structures and cognitive processes of the host's brain – the detection of integrity violations and the response to them may inherently be closely integrated,[15] insofar as the same artificial neurons that receive input through their synthetic dendrites that allows a violation to be detected will also be involved in transmitting output through their synthetic axons to the connected natural biological neurons in an effort to remedy the integrity violation.

B. Design of failure mode capacities and procedures

1. Design of the capacity to fail in a known state

Neuroprosthetic devices may be designed so that they fail (at least in the case of some kinds of failures) in a known state that preserves information about the devices' final pre-failure state.[16] It can be especially helpful for a neuroprosthesis to be designed to fail in a known secure state in cases when an implanted neuroprosthetic device cannot easily be inspected or otherwise immediately accessed to externally determine or confirm its failure state.[17]

2. Design of the capacity to fail secure

It is important that advanced neuroprostheses be designed to fail securely in the case of a failure of one of a device's boundary protection systems or components;[18] however, the basic concept of 'secure failure' may take on an unusual form in this context. Under normal circumstances, secure failure implies that after the failure of a boundary protection, information will be unable to either enter or leave a system until the failure has been remedied. In the case of neuroprosthetic devices, the state of secure failure may require

[15] Regarding integrated incident detection and response, see *NIST SP 800-53* (2013), p. F–226.

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

[17] See Chapter Three of this text for a discussion of issues relating to the lack of physical access to neuroprosthetic devices after their implantation.

[18] *NIST SP 800-53* (2013), pp. F–191-92.

that some information be able to enter and leave a device (or host-device system) in order to avoid causing direct physical or psychological harm to a device's human host.

Hansen and Hansen argue that in general, implantable medical devices should be designed in such a way that if an entire device, its individual components, or the larger system's security controls fail, they will 'fail open' in a way that allows rather than prevents the flow of information and access to the device, "since it is almost always better to give possibly-inappropriate access if the alternative is death or disability [...]."[19] In the case of a particular advanced neuroprosthetic device, it must be carefully investigated and determined whether failing into a state that is 'open' or 'closed' is more likely to lead to severe harm (or even death) for the device's host or operator under different kinds of possible circumstances. The types of information that should be allowed to enter or leave a device during failures should be determined by a device's designer in collaboration with physicians, psychologists, and biomedical engineers who possess relevant expertise about the potential physical and psychological impacts of device failure and a loss of information flow on a device's human host.

3. Design and installation of standby or backup components

Often the failure of a component triggers the automatic or manual transfer of the component's responsibilities to a standby component that was already in place and ready to be activated.[20] In the case of implanted neuroprosthetic devices whose ability to communicate with external systems cannot be reliably guaranteed, whose functioning depends on direct physical access to biological structures or processes within their host's body, or which cannot be easily manually accessed for repair or replacement, it may not be possible to utilize standby components that are located externally to a host's body: any standby components may need to be implanted into a host's body at the same time as the primary neuroprosthetic device or may need to be directly incorporated into the structure of that primary neuroprosthesis itself.

4. Design of the failover to standby or backup systems

The automatic switchover to an alternate system after the failure of an entire information system typically requires that mirrored systems or alternate processing sites[21] have already been established and adequately prepared and maintained in advance of the moment when the failure occurs. If by 'system' we understand an entire neuroprosthetic device, the unexpected failure of such a system may cause significant physical or psychological harm to the

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

[20] *NIST SP 800-53* (2013), p. F–231.

[21] *NIST SP 800-53* (2013), p. F–231.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

device's host or operator, especially if the device has critical health impacts. In some cases, it may not be possible to install an alternate system at the same time as implantation of the primary neuroprosthesis due to practical constraints such as space or power limitations or the fact that key biological structures and processes within the body of the primary device's host can interface with at most one device of that kind at a time.

In the case of 'failure' of an entire host-device system (e.g., through the incapacitation or death of a device's human host), there may not be any possibility of failover to an alternate information system, insofar as it is not feasible to 'mirror' in a synthetic external information system such traits as the unique physical, legal, and ontological identity or continuity of consciousness and agency of a particular human being, no matter how closely the external system may mimic some other traits displayed by the person (such as his or her genotype, physical appearance, or even the contents of his or her memory). While the concept of 'uploading' key information relating to a human being into an information system or creating physical or virtual copies of critical physical components or processes of the person has been proposed by some transhumanists and much debated[22] – and such techniques could indeed be said to provide a limited 'failover capability,' if the only goal is to preserve (partial and potentially inaccurate) records of some aspects of a human being's physical structure at a given point in time or of the person's past behavior – such mechanisms do not effect the continuation of a human being's essence or existence in any robust sense.

Perhaps the only way in which a neuroprosthetic device or neurocybernetic system could allow the continuation of the existence of a 'human being' through failover to an alternate information system would be if the individual were not a natural biological human being to begin with (in the way that the expression is traditionally understood) but were rather a simulacrum that was already, in some sense, a copy or representation without an original.[23] If the traditional understanding of the concept of a 'human being' were someday to be expanded or transformed to such an extent that an information system, virtual entity, software program, or instantiation of patterns within a neural network could be considered a 'human being' simply because it displays certain human-like characteristics or contains information derived from human

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

[23] See, e.g., Baudrillard, *Simulacra and Simulation* (1994), for a discussion of such issues from a philosophical perspective.

beings – without requiring that such information be housed within or accessed through a particular unique biological substrate – then it would be possible to imagine the preservation and continuation of an entire host-device system through failover to an entirely disjoint alternate system. However, such 'preservation' or 'continuation' is not at all the sort of preservation and continuation of personal consciousness, agency, and physical and noetic identity that a human being possessing a neuroprosthetic device would generally seek and which it may be the legal and ethical responsibility of the device's operator to ensure.[24]

5. Design of automatic device shutdown on audit failure

For some kinds of advanced neuroprostheses it may be essential that a device automatically shut down if its audit-processing ability is compromised (e.g., due to a hardware error or reaching the audit storage capacity), in order to avoid the possibility that the loss of audit-processing ability might allow the device to inflict physical or psychological harm on its host or others.[25] In other cases, a device may be required to continue operating after its audit-processing ability has been compromised and until it can be restored, due to the fact that the abrupt cessation of operations could inflict harm on its host or others.

C. Design of incident response mechanisms

1. Design of automated incident handling procedures

Relying on automated incident handling processes[26] to perform functions of incident detection, containment, and eradication may be hazardous if the execution of such functions is able or likely to directly or indirectly cause physical or psychological harm to a neuroprosthetic device's human host; an automated incident response system may not always recognize the effect that its efforts are inadvertently having on the device's host. On the other hand, in other situations, relying on an automated incident response system may be *less* likely to result in harm to a device's host than having human agents directly control the response, if the system can be trained to respond with a greater degree of speed, accuracy, and effectiveness than a human agent.

[24] See Proudfoot (2012). See also Chapter Three of this text for a discussion of the need to protect the personal identity, autonomy, agency, and sapient self-awareness of a neuroprosthetic device's human host.

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

[26] *NIST SP 800-53* (2013), p. F–105.

2. Design of dynamic reconfiguration as an incident response

Neuroprosthetic systems may be designed to dynamically reconfigure themselves either as a routine matter (in order to prevent potential attacks) or in response to an ongoing incident, in order "to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises."[27] In the case of neuroprosthetic devices utilizing biological components or physical neural networks, some degree of 'dynamic reconfiguration' may be continuously taking place.[28]

3. Design of dynamic information flow control as incident response

Particular kinds of information flow controls might be automatically enabled or disabled[29] if, for example, a neuroprosthetic device detects that its human host is experiencing a medical emergency or if the device's operator determines that the host is entering a situation in which specialized information flows are warranted.

4. Design of backup controls as incident response

A neuroprosthetic device may possess backup security controls (e.g., alternate methods for user authentication) that become active only if the device's primary controls have been compromised.[30]

5. Designing automated responses to denial of service attacks

Denial of service attacks[31] may take on new forms in the cases of some advanced neuroprosthetic devices. For example, a sensory neuroprosthesis such as an artificial eye could potentially be subjected to a successful denial of service attack by exposing it to an intense light source or array of light

[27] *NIST SP 800-53* (2013), p. F–105.

[28] For example, for a discussion of the ways in which long-term memories stored within the human brain can undergo changes in their nature and storage over time, see Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004). In a sense, memories stored within the brain's natural biological neural networks that undergo such changes (even if subtle ones) over time might be thought of as loosely analogous to metamorphic or polymorphic malware: a stored memory's ongoing dynamic reconfiguration may make it more difficult for adversaries to target that particular memory for alteration, manipulation, or deletion, if the storage location and identifying characteristics of the memory are not entirely stable. For factors that may either enhance or limit the dynamic reconfiguration of memories stored within the human brain, see, e.g., the discussion of holographic brain models in Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Westlake, "The possibilities of neural holographic processes within the brain" (1970); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web – The Correlation of Neuron Density with Brain Size" (1999).

[29] See *NIST SP 800-53* (2013), p. F–15.

[30] Regarding such controls, see *NIST SP 800-53* (2013), p. F–89.

[31] *NIST SP 800-53* (2013), p. F–187.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

sources that overwhelms, confuses, or blocks its ability to gather desired information from the environment. Denial of service attacks can also take the form of **resource depletion attacks** that attempt to exhaust the internal battery or other power source of an implantable neuroprosthesis by subjecting it to an unending string of wireless access requests from some external system: even if the neuroprosthetic device successfully rejects all of the unauthorized access requests, the work of responding to and verifying each request can quickly exhaust the device's battery and disable it.[32]

6. Determining the response to unsuccessful logon attempts

A control that automatically locks an account or delays the next logon prompt after a specified number of consecutive unsuccessful logon attempts[33] may be hazardous in emergency situations in which access to a device is needed immediately in order to prevent physical or psychological harm to its human host or others (and which may be precisely the sort of situation in which ongoing stress or physical impairment may cause the host's logon attempts to be unsuccessful).[34]

7. Design of the automatic wiping of a device in response to unsuccessful logon attempts

A control that automatically purges data from a neuroprosthetic device after a certain number or type of unsuccessful logon attempts may be desirable in order to preserve the confidentiality and possession of sensitive data stored within the device.[35] On the other hand, such countermeasures may be legally or ethically impermissible in situations in which they would cause physical or psychological damage to a device's host or to others.

8. Coordination of incident response processes with component suppliers

In some cases, successfully responding to an incident impacting an advanced neuroprosthesis may require coordination between the device's designer, manufacturer, OS and application developers, provider, installer, operator, and human host.[36]

[32] See the discussion of threats in Chapter Two of this text for more about resource depletion attacks.

[33] *NIST SP 800-53* (2013), p. F–21.

[34] See Chapter Three of this book for alternative methods for preventing resource depletion attacks involving a string of unsuccessful logon attempts, and see Chapter Two for a basic description of resource depletion attacks.

[35] Regarding the automatic wiping of devices, see *NIST SP 800-53* (2013), p. F–21.

[36] *NIST SP 800-53* (2013), p. F–106.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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 neuroprosthetic device 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. Activation of incident response mechanisms

1. Automated intrusion detection and response

The use of automated mechanisms to detect intrusions into a device or the surrounding body of its human host and to initiate particular response actions[37] must be undertaken carefully, insofar as some forms of intrusion (e.g., medical procedures) may be done with the host's consent and at his or her direct request, and automated responses could potentially cause physical or psychological harm if initiated while the host were in the midst of performing or undergoing some critical activity or otherwise at a time not desired by the host.

2. Detection and blocking of threatening outgoing communications

If viewed solely from the perspective of a neuroprosthetic device, **extrusion detection**[38] is essential for preventing potentially harmful traffic from passing from the device into the cognitive processes or biological systems of the device's human host. However, if viewed from the perspective of the larger host-device system, such controls are not extrusion detection but internal controls; true extrusion detection would attempt to detect and prevent, for example, the use of a neuroprosthesis by its host or operator to conduct unauthorized denial of service attacks, the dissemination of malware, illegal surveillance, or other illicit actions targeted at external systems or individuals.

B. Testing of incident response procedures

1. Use of simulated events for incident response testing

Incidents may be especially easy to simulate[39] for the host of a neuroprosthetic device when the device already creates a virtual or augmented reality

[37] Regarding automated intrusion detection and response mechanisms, see *NIST SP 800-53* (2013), p. F–131.

[38] *NIST SP 800-53* (2013), p. F–190.

[39] *NIST SP 800-53* (2013), p. F–104.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

for the host by supplying artificial sense data. At the same time, though, it may potentially be difficult for the hosts of such devices to distinguish simulated events from actual ones.[40]

2. Automated testing of incident response processes

Automated testing[41] may be necessary for neuroprosthetic devices that cannot directly be accessed by technologies or activities controlled by human agents but which may, for example, be accessible and potentially vulnerable to attacks utilizing nanorobotic swarms or other automated systems.

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

The fourth stage in the system development life cycle includes 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 performed 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. Flaw remediation

1. Centralized management of flaw remediation

Some kinds of 'flaws' detected in the functioning or operation of a neuroprosthetic device may be flaws not in the physical device or its software but in the structure and behavior of the larger host-device system in which it participates; in such circumstances, detection and remediation[42] of the flaw may depend largely on the individual capacities and action of the device's human host rather than the organizations responsible for designing, manufacturing, providing, or operating such neuroprostheses.[43]

2. Establishing deadlines and benchmarks for flaw remediation

In the case of some kinds of neuroprosthetic devices that interact with or support biological processes critical to the health of their human host, both

[40] See Chapter Four of this text for a discussion of the distinguishability of neuroprosthetically supplied information as an information security goal and attribute for neuroprosthetic devices.

[41] *NIST SP 800-53* (2013), p. F–104.

[42] Regarding centralized management of flaw remediation, see *NIST SP 800-53* (2013), p. F–216.

[43] See Chapter Three of this text for a discussion of the distinction between a neuroprosthetic device and its host-device system.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

legal, ethical, and operational considerations may dictate that a flaw must be corrected immediately upon its detection;[44] the fact that an organization works "as quickly as possible" to resolve the problem may not absolve it of responsibility for damage that occurs as a result. This is especially true in the case of devices that cannot easily be recalled, removed, or replaced if a flaw is discovered after a device has been implanted in its human host.[45]

3. Automatic updating of firmware and software to eliminate vulnerabilities

Allowing the automatic downloading, installation, and execution of operating system or application updates[46] by neuroprosthetic devices should only be undertaken after careful consideration, especially for devices with critical health impacts for their human host. The fact that operating system or application updates have undergone beta testing in a simulated development environment or with a limited number of host-device systems prior to their widespread public release may not ensure that the updates will not cause severe and unexpected negative impacts on the functioning of some implanted neuroprosthetic devices and harm for their human hosts, given the fact that the functioning of individual neuroprostheses may vary greatly depending on the unique nature of each device's physical interface with the neural circuitry of its human host and the nature of the host's cognitive patterns and activity.

B. Incident response

1. Use of detonation chambers for execution of suspicious code

The ability to implement a detonation chamber (or 'dynamic execution environment') within a neuroprosthetic device may be limited by the fact that some malicious code or applications may not be inherently (or obviously) harmful in themselves but only when allowed to interact with or be run by the cognitive processes of a particular human host. If it is not possible to simulate a host's cognitive processes with sufficient richness and accuracy in some artificial dynamic execution environment, then carrying out actions such as executing suspicious programs, opening suspicious email attachments, or visiting suspicious websites[47] within the detonation chamber may

[44] Regarding deadlines and benchmarks for flaw remediation, see *NIST SP 800-53* (2013), p. F–216.

[45] See Chapter Three of this text for a discussion of how the concept of zero-day vulnerabilities and attacks relates to neuroprosthetic devices – and especially to those possessing critical health impacts for their human host.

[46] *NIST SP 800-53* (2013), p. F–216.

[47] *NIST SP 800-53* (2013), p. F–214.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

not reveal the harmful effects that the same actions would have when performed by a neuroprosthetic device within a particular host-device system.[48]

2. Information spillage response

Care must be exercised in defining information spillage[49] with regard to neuroprosthetically augmented information systems and formulating spillage responses. For example, imagine that a human host possesses a neuroprosthetic device that stores information on flash memory that the host can access and 'play back' to his or her conscious awareness through sensory systems.[50] The host may have access and authorization to view classified information stored on the device, but viewing the information would create a (perhaps not entirely accurate) additional copy of the information in the natural biological long-term memory system within the host's brain; this could potentially be considered an information spillage. A similar situation would occur if a person were authorized to read printouts of classified information while in a secured location but not to transfer the information to a digital storage system; if the person's long-term memory processes were augmented with engram-storing mnemoprostheses, simply reading the documents in an authorized manner could result in the production of an unauthorized copy of the information within the neuroprosthetic system. In such situations, manual or automated responses that seek to take 'corrective action' to contain and eradicate spillage within the systems that have been 'contaminated'[51] by the information spillage have the potential to cause physical and psychological damage to a device's human host.

3. System recovery and reconstitution

The exact process of system recovery and reconstitution for a neuroprosthetically augmented information system will depend on the nature of the failure that has made the recovery process necessary and the extent of damage that the system and its stored information may have suffered. In the case

[48] Practical difficulties with implementing a detonation chamber within a neuroprosthetic device itself could arise either from the nature of the device's computing platform (e.g., it may be difficult or impossible to implement such an environment within a neuroprosthesis that does not execute traditional programs but instead processes information using a physical – and perhaps biological – neural network) or simply from limitations on the processing power, storage capacity, or power supply of a device's internal computer. See the device ontology in Chapter One of Gladden, *Neuroprosthetic Supersystems Architecture* (2017), for a discussion of such considerations.

[49] *NIST SP 800-53* (2013), p. F–109.

[50] For the idea of such sensory playback capabilities, see Merkel et al., "Central Neural Prostheses" (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

[51] *NIST SP 800-53* (2013), p. F–109-110.

of some kinds of neuroprostheses (e.g., those utilizing a complex physical neural network), it may theoretically be possible to scan and record the state of the entire device at a single moment in time – thus creating a backup file – however, there may be no mechanism available for restoring the system to a previous state by overwriting the device's current state with the information contained in the backup file.[52]

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 standard corrective and compensating 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. This concludes our investigation of preventive, detective, and corrective or compensating controls and their relationship to neuroprosthetic devices and neuroprosthetically augmented information systems.

[52] Regarding information system recovery and reconstitution, see *NIST SP 800-53* (2013), pp. F–87-88.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

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.

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

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.

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.

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-o/. 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*

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.

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.

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.

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

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

"Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.]

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. 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.

“Corrective and Compensating Security Controls for Neuroprosthetic Devices and Information Systems,” Chapter Eight in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 266-81. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).