Chapter Six

Preventive Security Controls for Neuroprosthetic Devices and Information Systems

Abstract. This chapter explores the way in which standard preventive 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.

Preventive controls considered include those relating to security planning; risk assessment and formulation of security requirements; personnel controls; information system architecture; device design principles; memory-related controls; cryptographic protections; device power and shutoff mechanisms; program execution protections; input controls; logical access control architecture; authentication mechanisms; session controls; wireless and remote-access protections; backup capabilities; component protections; controls on external developers and suppliers; environmental protections; contingency planning; system component inventory; selection of device recipients and authorization of access; physical and logical hardening of the host-device system and supersystem; device initialization and configuration controls; account management; security awareness training; vulnerability analysis; operations security (OPSEC); control of device connections; media protections; exfiltration protections; maintenance; security alerts; information retention; and media sanitization.

Introduction

In this chapter, we review a wide range of standard preventive security controls for information systems and identify unique complications and situations that arise from the perspective of information security, biomedical engineering, organizational management, and ethics when such controls are applied to neuroprosthetic devices and larger information systems that include neuroprosthetic components. The text provides an application of and commentary on 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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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]

Approaches to categorizing security controls

Some 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*, 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.[3] Here we instead utilize a classification of such measures as **preventive**, **detective**, or **corrective and compensating** controls. This chapter considers the first type of control, while the latter two types are investigated in the subsequent chapters.

Role of security controls in the system development life cycle

The preventive controls discussed in the following sections 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

[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).

[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 *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers* (2006), pp. 19-25. These are synthesized and applied 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).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

stage and the control's mechanisms are implemented in yet another stage. Here we have attempted to locate a control in the SDLC stage in which decisions or actions are undertaken that have the greatest impact on the success or failure of the given control. This stage-by-stage discussion of preventive 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. Security planning

1. Centralized management of security planning

In the case of neuroprostheses operated by organizations with relevant technical and managerial capacity, it is feasible to maintain a single coherent, organization-wide system for designing, implementing, and managing security controls and processes.[5] In the case of neuroprosthetic devices that are sold to the general public as consumer electronics devices, the host-device system constituted by an implanted device and its human host may not possess a single coherent, centrally-organized InfoSec approach but may instead reflect a patchwork of diverse and unrelated (and potentially contradictory) information security mechanisms and procedures developed by the device's manufacturer, its OS developer, the application developers of programs installed on the device, and the device's human host.[6]

2. Budgeting and allocation of financial resources

When considering information security for neuroprosthetic devices, special care must be given in the case of devices that will be permanently implanted and may reside within and interact with the biological systems and

[5] *NIST SP 800-53* (2013), p. F–144.

[6] See the device ontology in Chapter One of Gladden, *Neuroprosthetic Supersystems Architecture* (2017), and Gladden, "Managing the Ethical Dimensions of Brain-Computer Interfaces in eHealth" (2016), for a list of such relevant parties that can impact a neuroprosthetic device's information security, and see Chapter Five of this book for a discussion of the roles and responsibilities of such parties.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

cognitive processes of their human host for a period of years or decades – in order to ensure that a device's operator and (in a case in which the operator might declare bankruptcy, otherwise become incapable of providing InfoSec services, or otherwise fail in its obligation to ensure the long-term safety and information security of the implanted device) the device's human host will be able to provide the resources needed to ensure the safe and secure long-term functioning of the device.[7]

3. Planning of the system development life cycle

The system development life cycle[8] for neuroprosthetic devices should take into account the fact that once a device has been implanted in a human host, the organization operating the device may lose control over some or all aspects of the operations and maintenance phase and, in particular, the disposal phase for the device – insofar as it may not be legally, ethically, or practically feasible to carry out some kinds of activities (such as physically altering a device's integration with the neural circuitry of its human host or subjecting a device to removal or recall) without the host's consent.

4. Development of a system security plan

Development of an effective system security plan[9] for certain kinds of neuroprosthetic devices may be complicated by the fact that the human host in whom a device is implanted is either not aware of the device's existence or is not able – due to legal, ethical, or practical considerations – to participate constructively in execution of the system security plan. This may be the case, for example, in situations in which devices have been implanted in children, persons who are in a coma, or individuals who are otherwise incapacitated, as well as in the case of some devices used for military or intelligence-gathering purposes in which a host's access to information about a device and its operations must be constrained. Significant questions relating to personal privacy, human autonomy, bioethics, and the ethics of technology arise in such situations that must be addressed.[10]

5. Formulation of an information security architecture to support the enterprise architecture

An information security architecture is designed to describe in a clear and coherent manner "the overall philosophy, requirements, and approach to be

[7] Regarding the allocation of resources, see *NIST SP 800-53* (2013), p. F–156.

[8] See *NIST SP 800-53* (2013), p. F–157 for additional discussion of an SDLC in the context of information security.

[9] *NIST SP 800-53* (2013), pp. F–139-41.

[10] See Bowman et al., "The Societal Reality of That Which Was Once Science Fiction" (2012), for a discussion of some such issues.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

taken with regard to protecting the confidentiality, integrity, and availability of organizational information" and to explain "how the information security architecture is integrated into and supports the enterprise architecture."[11] For an advanced neuroprosthetic device, the information security architecture not only supports and is integrated into the overall enterprise architecture of the organization operating the device but must also incorporate (or, in effect, function as) the biomedical security architecture and cognitive and noetic security architecture of the human being in whom the device is implanted.

6. Formulation of a security concept of operations (CONOPS)

An organization's security concept of operations (or CONOPS) for an information system typically describes "how the organization intends to operate the system from the perspective of information security;"[12] any changes to the ongoing operations relating to the information system (and thus its CONOPS) will eventually be reflected in an updated system security plan, information security architecture, or other documents such as information security specifications governing specifications for future hardware and software acquisitions, SDLC materials, and systems engineering materials.[13] In the case of advanced neuroprostheses, the CONOPS may also draw on (and changes to the CONOPS may need to be reflected in):

- **Biomedical and bioengineering specifications** that set operating parameters that should be maintained within the biological organism of a device's human host in order to ensure its safe and effective functioning.
- **Biocybernetic system architecture** documents that describe the processes of communication and control within and between the device and its human host.
- **Cognitive and noetic security architecture** plans which describe and dictate the ways in which the privacy and autonomy of the mind of the device's human host (and the mind's integral cognitive processes) will be ensured.

7. Formalization of operations security (OPSEC) practices and personnel

Operations security (or OPSEC) attempts to secure an organization's sensitive information not directly through the development of access controls for the information itself but by ensuring more generally that the organization's operations do not unnecessarily disclose information that could be

[11] *NIST SP 800-53* (2013), p. F–142.
[12] *NIST SP 800-53* (2013), p. F–142.
[13] *NIST SP 800-53* (2013), p. F–142.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

used by adversaries to develop more effective means of attacking the organization and acquiring the sensitive information that they ultimately wish to obtain. OPSEC carries out its work through the "(i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures."[14]

In the case of advanced neuroprosthetic devices, the mandate of OPSEC practices and personnel may also need to be broadened to include not only preventing the unnecessary disclosure of information about an organization's internal operations but also preventing the unnecessary disclosure of information about the personal (non-organizational) activities of members of the organization who possess neuroprostheses, insofar as the sensitive organizational information contained in such devices could potentially be targeted through attacks that utilize avenues relating to members' private lives and activities.[15] At the same time, traditional OPSEC objectives of limiting the dissemination of information about the existence, purpose, use, and context of information systems may sometimes conflict with the desires of neuroprosthetic devices' human hosts, whom it may be legally and ethically difficult to prevent from disclosing information about their personal life and activities, should they desire to do so.

B. Risk assessment and formulation of security requirements

1. Criticality analysis of devices and components

In the case of an advanced neuroprosthetic devices, some device components might be designated as critical[16] not because they directly secure information contained within a device but because they support the physical and psychological health and safety of the device's human host, thereby indirectly ensuring the security of information held within the natural cognitive processes of the host's mind.[17]

---

[14] See *NIST SP 800-53* (2013), p. F–210, for a general description of OPSEC practices and personnel.

[15] See Chapter Three of this volume for a discussion of the ways in which a neuroprosthetic device is inextricably entangled with the larger host-device system in which it operates, through integration into the neural circuitry of its human host.

[16] *NIST SP 800-53* (2013), p. F–174.

[17] See Chapter Three of this text for the need to secure both a device and its larger host-device system. For the way in which a neuroprosthesis might enhance the information security of its host by, e.g., counteracting the effects of degenerative neurological conditions affecting memory and cognition, see Gladden, "Information Security Concerns as a Catalyst for the Development of Implantable Cognitive Neuroprostheses" (2016).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

2. Security categorization of the system and its information

For a neuroprosthetically augmented information system, security categorization[18] includes classifying the system and its information not only in relation to requirements determined by laws, regulations, and organizational policies and ethical standards relating to computer equipment but also in accordance with those regulations and guidelines that apply to personal health information, implantable medical devices, surgical procedures, psychological diagnostic and therapeutic procedures, and other relevant fields.[19]

3. Threat modelling and vulnerability analysis

In some cases, the ability of developers to perform effective threat modeling and vulnerability analysis[20] for advanced neuroprosthetic devices (or their constituent components or software) that are under development may be impeded by the fact that a device's functional and operational characteristics do not become clear until it is implanted in a particular human host and integrated with the host's neural circuitry, as a device may be largely passive in nature and its functional characteristics determined largely by the unique traits (e.g., memories, thoughts, or volitions) of the mind of its human host.[21]

4. Risk assessment

A risk assessment should be carried out (and updated as needed) for an information system as a whole as well as for relevant component devices and particular uses of the system, in order to analyze the "risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits."[22] Such assessments should identify both risks resulting from factors internal to the organization that will

[18] *NIST SP 800-53* (2013), p. F–151.

[19] For an overview of ethical issues with ICT implants – many of which are relevant for advanced neuroprosthetics – see Hildebrandt & Anrig, "Ethical Implications of ICT Implants" (2012). For ethical issues in information security more generally, see Brey, "Ethical Aspects of Information Security and Privacy" (2007). For regulatory issues, see Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); Mak, "Ethical Values for E-Society: Information, Security and Privacy" (2010); McGrath & Scanaill, "Regulations and Standards: Considerations for Sensor Technologies" (2013); and Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010).

[20] *NIST SP 800-53* (2013), p. F–175.

[21] See Chapter One of this text for a discussion of passive neuroprostheses and Chapter Three for a discussion of the classification of vulnerabilities and threats relating to advanced neuroprosthetic devices.

[22] *NIST SP 800-53* (2013), p. F–152.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

operate the device and internal to the device itself as well as risks resulting from external factors or agents.

In the case of advanced neuroprostheses, the risk assessment should not be limited to evaluating the potential impact of the unauthorized use or alteration of information contained within a device itself but also the impacts of the possible unauthorized use or alteration of information (such as memories or sense data) that are not contained within the physical components of the device but which are received, generated, transmitted, or stored by natural biological systems that belong to the device's human host and which are thus contained within the host-device system.[23]

5. Formulation of resource availability priorities and guarantees

Priority protection[24] may be utilized, for example, to ensure that a neuroprosthetic device's processes that control and enable the proper functioning of the respiratory and circulatory systems of its human host's body enjoy higher-priority access to the device's resources than processes that provide an augmented-reality enhancement to the user's vision that is useful but not critically necessary. Quotas[25] may be utilized to ensure that a particular process does not consume excessive resources, even when there is no other immediate demand for the resources; the use of such quotas can help ensure that spare resources are available for instantaneous access should they be required by another process (particularly a high-priority one) which needs the resources immediately in order to execute some critical task or prevent harm to a device's host or user.

6. Defining security requirements for the acquisition process

An organization's acquisition process for advanced neuroprostheses should not only define traditional functional, strength, and assurance requirements[26] relating to information security for a device itself but also for its larger host-device system. Goals for the host-device system also include preserving the cognitive and noetic security, privacy, and autonomy of the device's human host.

---

[23] See Chapter Three of this text for a discussion of information security for a device versus information security for its host-device system.

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

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

[26] Regarding the formulation of security requirements for the acquisition process, see *NIST SP 800-53* (2013), pp. F–158-60.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

C. Personnel controls

1. Separation of duties

Separation of duties[27] may be difficult to implement in cases in which a single person is both the operator and host of a neuroprosthetic device, as well as potentially the developer of applications or other content for use by the device. (Indeed, for some kinds of passive neuroprostheses, the brain of a human host may also be providing the 'operating system' for a device.[28])

2. Risk designations for positions

For advanced neuroprosthetic systems, the risk designation for positions[29] must take into account not only the extent to which a position's occupant will be able to directly access information stored within a device and within the natural biological systems of the device's human host but also the extent to which the position's occupant can indirectly alter, damage, or destroy information stored within the device or its host's biological systems by operating the device or interacting with its host in such a way that affects natural or artificial systems within the host's body that are not directly connected to the neuroprosthetic device but which can have an impact on the confidentiality, availability, or integrity of information stored within the device or its host. For example, the position of a technician who can alter a device's settings in such a way that causes the device's host to enter a comatose state may require a high risk designation, even if the position's occupant does not have any direct ability to retrieve or interpret information stored within the device or the host's natural memory systems.

3. Rules of behavior for organizational personnel

Under normal circumstances, the organization operating an information system may be able to unilaterally update the rules of behavior governing the use of that system and require all members of the organization to produce "a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior;"[30] an individual who declines to agree to the new rules of behavior may be denied access to the information system, removed from the organization, or potentially subjected to other disciplinary or personnel action as allowable by relevant law, regulations, employment agreements, and ethical guidelines. However, in the case of neuroprosthetic devices that have been implanted in the members of

[27] *NIST SP 800-53* (2013), p. F–18.
[28] See Chapter One of this text for a discussion of passive neuroprosthetic devices.
[29] *NIST SP 800-53* (2013), p. F–145.
[30] *NIST SP 800-53* (2013), p. F–141.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

an organization and are operated by that organization, it may be illegal, unethical, and impractical to attempt to force members to agree to new rules of behavior that are unilaterally imposed by the organization after devices have already been implanted; it may also be impermissible to attempt to deactivate or remove such devices simply because their hosts decline to agree to the updated rules of behavior.

4. Determining dual authorization for the execution of instructions

Controls that require the approval of two different authorized parties before instructions will be executed[31] may be impractical and inappropriate in the case of neuroprosthetic devices that are operated by their human host and which must be able to function when the host is in an open environment where a device cannot be accessed by other parties (e.g., a remote area without cell phone service or Internet access).

5. Personnel screening for access to confidential information

In the case of neuroprosthetically augmented information systems, it may sometimes occur that neuroprosthetic devices are used by their operating organization to gather classified or sensitive information that the device's human hosts are not themselves authorized to access or possess;[32] the legal and ethical conditions governing such activities should be carefully clarified.

6. Formalization of access agreements

Organizational access agreements may include components such as "nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements."[33] In the case of advanced neuroprosthetic devices, such agreements may be designed to protect the interests of multiple parties; for example, device designers and manufacturers, OS and software developers, and device operators may wish to ensure that devices' human hosts will not misuse information that they acquire through their possession of and interaction with the devices, and the devices' hosts may wish to ensure the confidentiality, possession, and legal ownership of sensitive information (e.g., relating to their biological or cognitive processes) that the devices may acquire or information (such as ideas, memories, inventions, discoveries, or artistic creations) that may be generated by the host's mind with the assistance of a device.

---

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

[32] Regarding personnel policies governing access to confidential information, see *NIST SP 800-53* (2013), p. F–146.

[33] *NIST SP 800-53* (2013), p. F–148.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

7. Formal indoctrination of personnel

Formal training for the hosts of neuroprosthetic devices regarding the legal and ethical frameworks governing the functioning of their devices and their relationships to classified or sensitive information may be necessary,[34] for example, if a host possesses an artificial eye or other neuroprosthesis that is continuously recording, uploading, and potentially making publically available information received from external environmental phenomena surrounding the host or from the host's internal cognitive processes.

8. Training against insider threats

In the case of neuroprosthetic devices that allow direct access to the cognitive processes (including sensory perceptions, thoughts, or memories) of their human host, complex legal and ethical questions arise over the proprietary of the accessing of such information by an organization's personnel in order to assess whether the host may constitute an insider threat to the organization's information security.[35]

9. Establishment of probationary periods

The use of probationary periods[36] for individuals receiving authorized access to information systems may not be legally, ethically, or practically feasible in the case of hosts in whom neuroprosthetic devices are being implanted. Any 'probationary period' designed to ensure a host's knowledge of and commitment to organizational policies (including InfoSec practices) may need to take place before the device is implanted and integrated into the host's neural circuitry, as it could be impossible to remove or deactivate the device after its implantation if the host should not successfully complete the probationary period. On the other hand, any probationary period designed to test a host's ability to successfully operate a device and use it to perform necessary InfoSec-related tasks may necessarily need to take place after the device has been implanted (and after the host has undergone any required recovery, adaptation, and training period), as it may be impossible to simulate operational conditions or to fully train and test the host in the device's use prior to the device's physical integration with the host's neural circuitry.

---

[34] Regarding InfoSec policies relating to the formal indoctrination of personnel, see *NIST SP 800-53* (2013), p. F–146.

[35] Regarding insider threats, see *NIST SP 800-53*, Rev. 4 (2013), p. F–38, and McCormick, "Data Theft: A Prototypical Insider Threat" (2008). See Chapter Two of this text for a discussion of other insiders within an organization who might pose a threat to a neuroprosthetic device's host or operator.

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

10. Establishing personnel sanctions for the violation of InfoSec policies

On the one hand, in order to ensure the security of highly sensitive information regarding the biological processes or cognitive activity of human hosts in whom neuroprosthetic devices are implanted, it may be necessary to enact a stringent formal sanctions[37] process to discipline individuals within an organization who disregard or violate established InfoSec procedures. On the other hand, there may be significant legal and ethical issues that complicate an organization's ability to discipline the human host of a neuroprosthetic device who violates organizational information security procedures, especially if those procedural requirements have been unilaterally imposed by an organization subsequent to a device's implantation or otherwise enacted without the full informed consent of the device's host.

11. Establishing personnel termination procedures

Standard procedures upon termination of the employment of an organization's member may include action by the organization that "Disables information system access" previously enjoyed by the employee within a specified time period, "Terminates/revokes any authenticators/credentials associated with the individual," "Retrieves all security-related organizational information system-related property," and "Retains access to organizational information and information systems formerly controlled by terminated individual."[38] The ability of an organization to carry out such actions in the case of an organizational information system that takes the form of a neuroprosthetic device implanted in a (former) employee may be significantly constrained by legal, ethical, and practical considerations.

For example, even if an employee had signed an employment contract or agreement clearly specifying that any devices subsequently implanted in the employee by the organization (and all information contained within them) were property of the organization and that the organization enjoyed the right to reclaim such devices at information any time, the ability of the organization to enforce the agreement and reclaim an implanted device through forcible surgical extraction would be legally and ethically doubtful, at best – although the employee could potentially be subject to civil action for theft or conversion. Moreover, even if it is technologically possible for an organization to execute such actions by sending remote instructions to a device, the organization may not have a legal or ethical ability to forcibly reclaim a neuroprosthetic device or to destroy all of the information contained on it (such

[37] *NIST SP 800-53* (2013), p. F–150.
[38] *NIST SP 800-53* (2013), p. F–147.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

as thoughts or memories of the device's host), even if an employment agreement were unilaterally breached or terminated by the device's host in contravention of the agreement's terms and conditions.

12. Establishing post-employment obligations of personnel

Automated systems may be employed to ensure that former employees are, for example, not able to make use of classified or sensitive information contained within implanted neuroprostheses that had been provided to them by their former employer for work-related purposes, or even to utilize the devices at all.[39] If a neuroprosthetic device has been designed and constructed in such a way that ongoing proactive authorization or support from the organization employing the device's host (e.g., wireless signals sent to the device from an external organizational information system) are required in order for the device to function or for its contained information to be accessible, the withdrawal of such authorization upon termination of an employee may constitute a practice that is legally and ethically permissible, provided that it does not have a negative impact on the employee's psychological, physical, or social wellobeing. In its natural state (i.e., in the absence of such authorization signals) the device will simply become nonfunctional, and the organization has no obligation to provide such authorizations.[40] On the other hand, the situation becomes more legally and ethically complex if an implanted neuroprosthetic device's natural state is one in which the device functions nominally and information contained within it is available to the device's host, and the functioning of the device (and availability of its contained information) can only be suppressed by the organization through the ongoing application of some proactive measure – such as bombarding the host's body with electromagnetic impulses that jam the device's communications or otherwise disrupt its operation. The legal, ethical, and practical ability of an organization to carry out such measures to impair the operation of an implanted neuroprosthesis may be severely constrained.

[39] Regarding post-employment requirements relating to information security, see *NIST SP 800-53* (2013), p. F–147.

[40] See the discussion in Chapter Three of this text of proposed schemes that utilize external hardware tokens, cloaking devices, or gateway devices whose presence causes an implanted medical device to behave in a particular way during emergency (or non-emergency) situations. Employers could potentially develop similar systems in which an employer could disable an implanted neuroprosthesis or cause it to 'fail closed' not by physically accessing the device or even wirelessly sending the device a command to disable itself (which may not be legally or ethically possible) but simply by confiscating, disabling, or failing to renew some external token or device in the possession of the implanted neuroprosthetic device's host that is needed in order to prolong the functioning of the implanted device.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

D. Designing an architecture for the entire information system

1. Development of comprehensive information system documentation

An organization must acquire and appropriately secure documentation from a neuroprosthetic device's designers, manufacturers, and OS developers regarding subjects such as high-level design principles, low-level design details, the functional properties of security controls built into the device and its OS, source code, external system interfaces, and the full characteristics of administrative accounts built into the device and its OS.[41] In the case of an advanced neuroprosthesis, such documentation would also include recommendations and requirements regarding the biological systems and structures into which the device will be integrated, recommended methods for performing implantation and integration of the device into the host's neural circuitry, and circumstances in which implantation of a device into a particular host is contraindicated or deactivation or removal of the device would be required.

2. Intentional heterogeneity of systems, devices, and components

Increasing the heterogeneity and diversity of the sources, forms, functionalities, and procedures relating to the individual components of neuroprosthetic devices or the larger information systems that incorporate them is a double-edged sword: on the one hand, such diversity "reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks."[42] On the other hand, increased heterogeneity and diversity of systems and components may contravene the InfoSec principle of utilizing conceptually simple design and may increase the cost, complexity, and difficulty of properly managing information systems.[43]

3. Planning of connections to non-organizationally owned systems and devices

Neuroprosthetic devices may operate within a complex context in which, for example, key components of a device are owned by an organization but other components consist of biological matter that is a part of a host's body. This may complicate the process of establishing controls for the sharing of information with components or systems that are not owned by the organization.[44]

---

[41] *NIST SP 800-53* (2013), pp. F–160-61.

[42] *NIST SP 800-53* (2013), p. F–204.

[43] *NIST SP 800-53* (2013), p. F–204.

[44] Regarding non-organizationally owned systems, devices, and components, see *NIST SP 800-53* (2013), p. F–33.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

4. Analysis of the reliance on external information systems

Insofar as the information within a neuroprosthetically augmented information system can be accessed by the mind of a device's host, it is possible (and in some situations perhaps likely) that the information will eventually be transmitted to or copied – in a manner that may or may not accurately represent the original source information – into external information systems to which the host's mind has access (such as the host's personal computer, smartphone, or other systems).[45]

5. Planning of boundary protection for physical, psychological, and logical boundaries

Boundary protection is of critical importance for advanced neuroprosthetic devices and takes on new meanings in this context. An information system should monitor (and, as appropriate, control) all communications taking place at the system's external boundary which cause data to enter or leave the system as well as communications taking place across key internal boundaries within a system or its constituent components.[46] In the case of advanced neuroprosthetic devices, key boundaries include the:

- Physical boundary between a neuroprosthetic device and the biological matter of its human host (and in particular, the physical boundary or interface between the device and natural biological neurons within the host's body).[47]
- Physical boundary between a neuroprosthetic device and the environment external to its host's body (for prostheses that are exposed to the external environment). This may include a boundary with particular systems, devices, or individuals located within that external environment.
- Physical boundary between a host's body and the surrounding external environment.[48]
- Physical boundary between a neuroprosthetic device and other implanted devices within its host's body.

[45] Regarding the use of external information systems, see *NIST SP 800-53* (2013), p. F–32.

[46] *NIST SP 800-53* (2013), p. F–188.

[47] See Chapter One of this text and the device ontology in Chapter One of Gladden (2017) for a discussion of different kinds of neural interfaces.

[48] For a discussion of the significance of the physical boundaries of a human organism and the ways in which technologies such as implantable neuroprostheses can impact cognitive processes and the "moral sense of person" versus "the notion of person as a subject of experiences," see Buller, "Neurotechnology, Invasiveness and the Extended Mind" (2011).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

- Physical, physiological, psychological, and logical boundaries between different neuronal processes within a host-device system – such as the boundary at which environmental stimuli are transduced into electrochemical signals by sensory organs and the boundary at which raw sense data is transformed into sensory perceptions within the host's mind. Also included are psychological boundaries between phenomena such as memory, emotion, volition, and conscience whose phenomenological[49] and experiential boundaries as seen from the perspective of the mind of a device's human host may not clearly correspond to physical boundaries within the host-device system.

Some neuroprosthetic devices may interact with their human host only through a small number of managed interfaces (e.g., synaptic connections through which signals are received and transmitted); other devices, such as those composed of biological material, may interact with a device's host through unmanaged interfaces that may change significantly over time as a result of the growth of biological components of the device, changes in the host's organism, or both. It may be appropriate and desirable to create outward-facing subnetworks (or '**demilitarized zones**') that are separated physically or logically from a device's internal networks[50] and which interface either with the biological systems and cognitive processes of the device's human host, with supplemental prostheses or other accessories that can be connected to the device (e.g., through generic ports or sockets), with the external physical environment (e.g., to prevent sensory overload or 'sense hacking' that could occur if the external environment supplied stimuli directly to internal systems), or with other external systems such as Wi-Fi networks and the Internet.

6. Planning of internal system interconnections

If multiple kinds of neuroprostheses are available for acquisition, installation, and use by members of the general public as consumer electronics devices, it may be difficult or impossible to predict the ways in which multiple devices may be combined and interconnected within a single human host. Even if devices do not directly interconnect with one another, they may indirectly interconnect through the host's brain and mind, which can serve as a bridge allowing information to flow between devices and influence one another.[51]

---

[49] See Chapter Two of Gladden (2017) for an analysis of such boundaries from a biocybernetic perspective. For an exploration of phenomenological issues, see Heersmink, "Embodied Tools, Cognitive Tools and Brain-Computer Interfaces" (2011).

[50] *NIST SP 800-53* (2013), p. F–188.

[51] Regarding system interconnections, see *NIST SP 800-53* (2013), pp. F–57-58.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

7. Planning the physical partitioning of the information system

Typical approaches to information system partitioning[52] – such as physically separating different components in different racks within the same room, in different rooms, or in wholly different geographical locations – may not be feasible in the case of an implantable neuroprosthetic device that must be as small and compact as possible. It may be possible to physically separate components through the creation of body area networks (BANs) or body sensory networks (BSNs)[53] whose components are distributed throughout a host's body and interact with one another wirelessly. It may also be possible to separate the implantable device from external devices or support systems that communicate with the implantable device; however, care must be taken to ensure that the implanted portion of the system can continue to operate in a way that will not create the danger of physical or psychological harm for the device's host or others if the device should temporarily or permanently lose the ability to communicate with the external systems (e.g., because the device's host has entered a building whose construction blocks the transmission of wireless signals).

8. Planning of hardware separation

Hardware separation mechanisms[54] may be utilized, for example, to segregate the systems of a neuroprosthetic device that interact directly with the neural circuitry of the device's host from those which relate to the device's power supply or wireless communication with external support systems.

9. Planning of application partitioning

Separating a system's user functionality and interface services from its administrative and system management functionality[55] may be difficult or impossible in the case of a neuroprosthetic device whose human host is also its operator. In other cases, such partitioning may be not only desirable but necessary – for example, if a device's host is the 'user' responsible for controlling some aspects of the device's ongoing operation but management of key med-

[52] *NIST SP 800-53* (2013), p. F–207.

[53] See Ullah et al., "A Study of Implanted and Wearable Body Sensor Network" (2008); Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012); and Li et al., "Advances and Challenges in Body Area Network" (2011).

[54] *NIST SP 800-53* (2013), p. F–185.

[55] *NIST SP 800-53* (2013), p. F–184.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

ical and technical aspects of the device's behavior is controlled by remote 'users' in the form of a team of specialized medical and IT personnel who possess expert knowledge that the human host lacks.[56]

10. Determining an architecture for device name and address resolution

Particularly in the case of a neuroprosthetic system that includes multiple devices implanted within a single human host that must communicate with one another,[57] it may be appropriate and desirable to utilize separate name and address resolution services[58] (such as those offered by DNS servers and network routers) for processing internal information requests from the component devices that constitute the system and external information requests from external networks such as the Internet.

11. Designing host-client device systems

In the sense commonly employed within the field of IT management, the word 'host' does not refer to the human being in whom a neuroprosthetic device is physically implanted but to a device (such as a server or desktop computer) that executes some piece of software and potentially serves as a host in a host-client device system.[59] In the case of an organization that has deployed many neuroprosthetic devices among its personnel, the organization may operate a centralized information system housed within a secure organizational facility that serves as the host for the client neuroprosthetic devices. If all of the client devices are monitored or controlled by, receive software updates from, or are otherwise affected by the centralized system, the use of effective security controls to protect that core system is important for securing its client devices.

12. Planning of collaborative computing capacities

Advanced neuroprosthetic devices may be able to serve directly as collaborative computing devices;[60] for example, an artificial eye implanted in one human host could potentially stream live video that can be viewed by other persons in order to share in the host's visual experiences. Similarly, a human host possessing a body with robotic cybernetic limbs might allow a professional dancer to take temporary control of the body in order to create a form of shared performance art. Possibilities also exist for the internal cognitive

[56] See Chapter Three of this text for a discussion of the distinction between a neuroprosthetic device's human host and its user or users.

[57] Body area networks and body sensor networks typically constitute such systems. See Ullah et al. (2008); Cho & Lee (2012); and Li et al. (2011).

[58] *NIST SP 800-53* (2013), p. F–201.

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

[60] *NIST SP 800-53* (2013), p. F–197.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

processes of neuroprosthetic devices' hosts to form collaborative computing devices by creating 'hive minds' or communities of individuals whose minds are linked through their implanted neuroprostheses.[61] A neuroprosthetic device may also allow its human host new ways of accessing, controlling, and obtaining information from traditional collaborative computing devices such as cameras, microphones, or printers. The growth of the Internet of Things and new kinds of devices such as 3D printers and smart homes creates entirely new types of networked systems that can potentially be accessed and controlled by means of neuroprosthetic devices.[62] All of these possibilities raise significant questions of information security both for the users and operators of neuroprosthetic devices and for other individuals who use the collaborative computing devices or can be affected by their activities.

13. Planning for information in shared resources

Care must be given to ensuring information security in situations in which other users, accounts, or processes may have access to shared system resources through which information created or used by or otherwise related to a neuroprosthetic device has passed or within which it has been stored. In such circumstances, information security is pursued through the control of **object reuse** and **residual information protection**.[63] Similar but distinct concerns include the need to address situations of **information remanence** in which action has been undertaken to erase or destroy information (and it may nominally be designated by a system as 'deleted') but residual traces of the data still exist and can potentially be accessed,[64] as well as situations in which **covert channels** are utilized to access, transmit, or manipulate information in ways

[61] The prospect of creating 'hive minds' and neuroprosthetically facilitated collective intelligences is investigated, e.g., in McIntosh, "The Transhuman Security Dilemma" (2010); Roden, *Posthuman Life: Philosophy at the Edge of the Human* (2014), p. 39; and Gladden, "Utopias and Dystopias as Cybernetic Information Systems: Envisioning the Posthuman Neuropolity" (2015). For critical perspectives on the notion of hive minds, see, e.g., Maguire & McGee, "Implantable brain chips? Time for debate" (1999); Bendle, "Teleportation, cyborgs and the posthuman ideology" (2002); and Heylighen, "The Global Brain as a New Utopia" (2002).

[62] See Evans, "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World" (2012); Merkel et al., "Central Neural Prostheses" (2007); and Gladden, "Neural Implants as Gateways to Digital-Physical Ecosystems and Posthuman Socioeconomic Interaction" (2016).

[63] *NIST SP 800-53* (2013), p. F–186.

[64] With regard to the case of information stored within a physical neural network – and perhaps even within the human brain's natural biological long-term memory storage systems – researchers have had some success with attempting to manipulate or delete specific memories stored within the brains of mice; see, e.g., Han et al., "Selective Erasure of a Fear Memory" (2009). However, it is unclear to what extent, if any, it might someday be possible to 'delete' or 'erase' complex

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

that bypass information flow restrictions – potentially by employing a device's systems, components, or processes in imaginative or counterintuitive ways that were never anticipated by a device's designer.[65]

For some neuroprosthetic devices, 'shared resources' may include biological systems of a device's human host (such as the circulatory system, sensory organs, or limbs) or the host's cognitive systems and processes (such as natural memory storage systems and particular mnemonic content); the use of a neuroprosthetic device may create traces of information in such shared systems that can be accessed by other processes or users of the device or other implanted devices within the host's body, even if they lack direct access to components, user accounts, or processes within the neuroprosthetic device that created the original information.

14. Planning of offline storage

For some kinds of implantable neuroprosthetic devices (e.g., those that store information within an internal physical neural network or which lack mechanisms for transmitting information to or receiving information from external systems), a device itself and its own internal storage mechanisms may constitute a form of off-line storage, insofar as the information is not accessible from any sort of external networks.[66]

15. Planning of out-of-band channels

For human beings possessing certain kinds of neuroprosthetic devices, such a device may provide a new kind of 'out-of-band channel'[67] for conveying information directly to the conscious awareness or cognitive processes of its human host in a way that bypasses or avoids the traditional biologically based 'in-band channels' comprising sensory organs. Conversely, for the human host of a sensory or cognitive neuroprosthesis who ordinarily receives sensitive or secure information through the device (e.g., with information being presented in the host's visual field through use of augmented reality or being directly incorporated into the host's short- or long-term memory), receiving information through the use of the host's natural biological sensory organs may constitute the use of an out-of-band channel.

---

long-term memories stored within the natural long-term memory systems of human brains; information remanence may thus become a major challenge for neuroprosthetic devices utilizing physical neural networks, biological components, and engrams for the storage of information. Such issues surrounding the possibility of deleting long-term memories may become even more vexing if, e.g., holographic or holonomic models of the brain's memory systems are correct.

[65] *NIST SP 800-53* (2013), p. F–186.

[66] Regarding offline storage, see *NIST SP 800-53* (2013), p. F–204.

[67] For the InfoSec implications of out-of-band channels, see *NIST SP 800-53* (2013), pp. F–209-10.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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. General device design principles

1. Formal InfoSec policy modelling for design of a device, system, and supersystem

The kinds of formal policy modelling tools traditionally used to model practices such as nondiscretionary access control policies with formal languages[68] may have limited applicability for some kinds of advanced neuroprostheses. For example, some kinds of neuroprosthetic devices that comprise physical neural networks or swarms of nanorobotic elements may not include nondiscretionary access controls that can easily be modelled; in the case of devices that are passively controlled by the minds and cognitive processes of their human hosts, a system's security controls may be entirely discretionary and controlled by the decision-making and volition of the device's human host. It may be possible to develop new kinds of formal policy models and modelling languages that address the unique information security situations of advanced neuroprosthetic devices (including the typically important goal of preserving autonomy and agency for the host-device system as a whole).

2. Updating of security engineering principles

In developing the designs and specifications for advanced neuroprosthetic devices, entirely new kinds of information system security engineering principles[69] may need to be developed that incorporate considerations relating to cognitive and noetic security and the preservation of human agency and autonomy within a host-device system.

3. Pursuit of trustworthiness through security functionality and assurance

The trustworthiness[70] of an information system depends both on the (1) set of features, mechanisms, and procedures built into constituent devices

[68] *NIST SP 800-53* (2013), p. F–178.
[69] *NIST SP 800-53* (2013), p. F–162.
[70] *NIST SP 800-53* (2013), p. F–173.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

and the operating environment that together constitute the system's *security functionality* and (2) the *security assurance* that allows an organization to believe that the potential benefits offered by the security functionality are actually being obtained through a proper and effective implementation of the functionality.[71]

It should be noted that in at least some respects, some kinds of advanced neuroprostheses may be inherently *untrustworthy*. For example, certain kinds of devices that include a physical neural network and which interact closely with the natural memory systems of the human mind to expand or support the mind's long-term memory storage may be subject to the same kind of mnemonic compression, distortion, and gradual information degradation that is observed with natural human memories.[72]

4. Use of conceptually simple design

Requirements that developers develop systems that utilize "a complete, conceptually simple protection mechanism with precisely defined semantics"[73] may be difficult to realize in situations in which protection mechanisms may, for example, be implemented and directed largely in a discretionary manner by the mind of the human host in whom a device is implanted.

5. Design of coupled and cohesive security function modules

It is a best practice to develop and utilize "security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules."[74] In the case of highly sophisticated multimodal neuroprosthetic devices, it may be possible to develop individual security functions that separately address, for example, security relating to incoming sense data (with data from each sensory organ handled separately), internal cognitive activities (with each activity possessing its own security functions), and outgoing motor instructions (with different security functions for each motor modality and effector. The development of independent modules may not be possible with other kinds of neuroprosthetic devices, such as those that utilize a physical neural network or which store and process information holographically.

---

[71] *NIST SP 800-53* (2013), p. F–173.

[72] For a discussion of such issues, see Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

[73] *NIST SP 800-53* (2013), p. F–179.

[74] *NIST SP 800-53* (2013), p. F–186.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

6. Planning non-persistence and the regular refreshing of devices and components

Rather than waiting until it has been detected that particular components or services have been compromised and then replacing them, terminating their functionality, or otherwise addressing the situation, an organization may proactively refresh components and services at regular or random intervals. Such procedures can reduce the effectiveness of certain kinds of **advanced persistent threats** (APTs) that must have access to or operate within a particular computing environment for a substantial period of time in order to successfully exploit vulnerabilities and complete their attack.[75] For some kinds of neuroprosthetic devices, non-persistence may be difficult to implement, insofar as a device must provide continual service and 100% availability in order to avoid causing physical or psychological harm for its host or operator, and the time and actions needed to refresh components or services would cause an impermissible interruption or disruption to the device's functionality.[76] In other cases, it may be possible to refresh components or services during non-critical moments (e.g., when a device's host is asleep or not engaging in particular kinds of activities). Other kinds of neuroprosthetic devices (such as those utilizing biological components or neural networks) may neither require nor allow such periodic refreshing of components or services.

7. Planning physical and logical separation of information flows

For some kinds of neuroprostheses (e.g., those utilizing physical neural networks) it may be extremely difficult to segregate different kinds of information moving through the devices.[77]

8. Denial of inbound and outbound communications by default

The practice of denying all inbound and outbound network communications traffic by default and allowing it only after it has been approved as an

[75] *NIST SP 800-53* (2013), p. F–232.

[76] See Chapter Three of this text for a discussion of neuroprosthetic devices for which 100% availability is required and any downtime presents a major hazard.

[77] For example, if various holographic or holonomic models of the human brain's cognitive processing and memory storage are correct, it may be difficult or impossible to isolate a certain small group of neurons as completely 'containing' a particular memory or thought. For discussion of such issues, see, e.g., 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). An overview of conventional contemporary models of long-term memory is found in Rutherford et al., "Long-Term Memory: Encoding to Retrieval" (2012). Regarding separation of physical and logical information flows, see *NIST SP 800-53* (2013), p. F–18.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

exception[78] may not be possible for some kinds of neuroprosthetic devices. For example, in the case of sensory neuroprosthetics receiving sensory stimuli from the environment, it may not be feasible or theoretically possible to apply filters or tests at the boundary between the external environment and the device to determine with any accuracy what the ultimate effect of the sense data may be on the psychological health and security of a device's host and thus to allow only certain information to be transmitted inward for further processing and utilization by the device and host-device system.

9. Design of devices as thin nodes

It may be difficult to implement many kinds of neuroprosthetic devices as thin nodes,[79] given the diverse range of complex tasks that such devices must perform; the multiple forms of communication and interaction that they may need to carry out with biological systems, other implanted devices, and external support systems; the high standards set for their functionality; and the fact that such devices may need to be engineered with a wide range of surplus capacities that may or may not ever be used, due to the difficulty of modifying devices to increase their capacities after their implantation in a human host. On the other hand, some kinds of passive neuroprostheses[80] may function as thin nodes if they are designed to be directly controlled by the biological processes of their human host and do not need to possess sophisticated mechanisms for the storage of digital data, wireless communication, or other functionality commonly found in mobile devices.

10. Planning of distributed processing and data storage

Some kinds of neuroprosthetic devices (such as those employing a physical neural network with holonomic or holographic storage models) may inherently utilize distributed processing and storage.[81]

11. Restricting the use of live data during system development

The use of live data during the development and testing of information systems is generally discouraged, as storing information within systems whose security functionality is not yet assured and utilizing the information in a way unprotected by an organization's existing InfoSec mechanisms and procedures creates a significant risk.[82] However, with some kinds of neuro-

[78] *NIST SP 800-53* (2013), p. F–189.

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

[80] See Chapter One of this text for a discussion of passive neuroprosthetic devices.

[81] Regarding distributed processing and data storage, see *NIST SP 800-53* (2013), p. F–209.

[82] *NIST SP 800-53* (2013), p. F–176.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

prosthetic devices it may be impossible to avoid the use of live data even during the initial development and testing phases – for example, in cases in which a neuroprosthetic device is not fully assembled in an external facility and then implanted whole into the body of a human host but is instead assembled (or, if it utilizes biological components, even 'grown'[83]) within the body of its human host, piece by piece – perhaps through the use of nanorobots[84] or other technologies. In such cases, the development process for each particular neuroprosthetic device is unique and depends on (and is guided by) the immediate feedback provided by live data generated by the cognitive or biological processes of the device's human host.

B. Memory-related controls

1. Memory protection

Traditionally, memory protection involves hardware- or software-enforced practices such as ensuring that adversaries are not able to execute code in non-executable areas of memory.[85] In the case of advanced neuroprosthetic devices, it is not only the executable memory of a device's electronic components that must be protected but also the sensory, short-term, and long-term memory of the device's human host and any memory systems that may be created by the device and host acting jointly within the host-device system.[86] For example, cyberattacks that are able to manipulate sensory memory could potentially cause the host to perform (or not perform) physical actions in a particular manner desired by an adversary, by distorting the host's understanding of his or her environment, bodily position, or other phenomena; manipulated or fabricated information contained within sensory memory would then compromise the host's short- and long-term memory after being transmitted to those systems. Directly manipulating a host's long-term memory could also cause the host to execute or not execute actions as desired

[83] For the possibility of neuroprosthetic devices involving biological components, see Merkel et al. (2007). For a hybrid biological-electronic interface device (or 'cultured probe') that includes a network of cultured neurons on a planar substrate, see Rutten et al., "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe" (2007). Hybrid biological-electronic interface devices are also discussed in Stieglitz, "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems" (2007).

[84] See Pearce, "The Biointelligence Explosion" (2012).

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

[86] For experimental research with mice that suggests the possibility of eventually developing human mnemoprostheses, see Han et al. (2009) and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013). For the possibility that an adversary might use a compromised neuroprosthetic device in order to alter, disrupt, or manipulate the memories of its host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

by an adversary – for example, pressing a button that the host's long-term memory tells the host will have one effect, when in fact pressing the button will have a completely different effect, and the host's memory of the button's significance has been altered.

Note that there are systems and processes found (or whose existence is hypothesized) within the human mind that play roles analogous to those of the executable memory found in a traditional computer and which relate to human memory but may also involve other kinds of processes – for example, the visuospatial sketchpad described in the Working Memory model[87] or the spotlighted 'theater of consciousness' described in the Global Workspace Theory.[88]

2. Design of protections for information at rest

The phrase '**information at rest**' is generally used to describe information during those times when it is physically embodied in a particular way that is seen as relatively stable – namely, it describes "the state of information when it is located on storage devices as specific components of information systems."[89] In reality, even information that is stored on physical storage devices of the most reliable and secure form imaginable is never truly 'at rest,' as the physical substrates within which information is stored (such as the ferromagnetic layer of a hard disk drive's platter) are continuously being impacted at the subatomic level by phenomena such as cosmic rays and probabilistic quantum effects, even if these phenomena rarely have impacts that are directly visible at the macroscopic level. In well-designed systems, this process of ongoing change at the subatomic level in the structure and composition of the substrates typically does not modify the contents of the information as it is accessed and interpreted by human beings; nonetheless, it has the potential to do so. The possibility that even 'information at rest' could be modified or destroyed through the impact of 'soft errors' caused by cosmic rays, other electromagnetic radiation, or random quantum effects generally increases as units of data (such as bits) are stored in smaller physical structures, such as those of a single electron.[90]

---

[87] See, e.g., Baddeley, "The episodic buffer: a new component of working memory?" (2000).

[88] See, e.g., Baars, *In the Theater of Consciousness* (1997).

[89] *NIST SP 800-53* (2013), p. F–203.

[90] For a discussion of various kinds of soft errors and approaches for preventing them or limiting their impact, see Borkar, "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation" (2005); Wilkinson & Hareland, "A cautionary tale of soft errors induced by SRAM packaging materials" (2005); Srinivasan, "Modeling the cosmic-ray-induced soft-error rate in integrated circuits: an overview" (1996); and KleinOsowski et al., "Circuit design and modeling for soft errors" (2008).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

For some kinds of neuroprosthetic devices that utilize biological material for storing information, new complications are added to this picture: 'information at rest' that is stored within the patterns of activity of living cells (or within DNA[91]) may be modified or destroyed over time due to the birth, growth, mutation, or death of cells or the alteration of DNA due to radiation, chemical agents, biological agents and vectors, or other factors.

C. Cryptographic protections

1. Design of cryptographic protections and keys

When attempting to secure certain kinds of neuroprosthetic devices, it may be possible (or even necessary) to develop entirely new kinds of encryption which, for example, use the unique memories or other contents of the cognitive processes of a human mind as cryptographic keys.[92]

2. Planning of cryptographic key management

The need to maintain possession and confidentiality of and access to cryptographic keys[93] that are necessary for the effective functioning of a neuroprosthetic device becomes even more critical if failure or unauthorized use of the device has the potential to cause physical or psychological harm to the device's user or others.[94] The **escrowing** of encryption keys may be a necessary practice but also one that must be carried our carefully – especially if a neuroprosthetic device contains components dependent on the encryption key which, due to their implantation in the host's body, cannot easily be updated, otherwise modified, or replaced if the key should be lost or disclosed to unauthorized parties.

---

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

[92] For such possibilities, see Thorpe et al., "Pass-thoughts: authenticating with our minds" (2005); Mizraji et al., "Dynamic Searching in the Brain" (2009), where the term 'password' is used in a more metaphorical sense than the typical meaning in information security, although the dynamic memory searching mechanisms described there could potentially also serve as the basis for an authentication system; and Gladden, "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values" (2015). Regarding cryptographic protections, see *NIST SP 800-53* (2013), p. F–196.

[93] *NIST SP 800-53* (2013), p. F–195.

[94] See Chapter Three of this text for proposed approaches to storing the cryptographic key for an implanted neuroprosthetic device on the host's body in the form of an external token, bracelet, tattoo, or other item, in order to provide device access to medical personnel in the case of a medical emergency affecting the device's host.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

3. Full-device encryption

Although desirable from an InfoSec perspective, full-device encryption and container-based encryption[95] may not be possible for the contents of some kinds of neuroprosthetic devices, such as those storing information in a physical neural network.

4. Planning encryption of outgoing device transmissions

Encrypting outgoing transmissions[96] may be impossible, for example, in the case of neuroprosthetic devices that transmit information in the form of electrochemical signals that must be interpretable by natural biological neurons within the body of a device's host; in such cases, a device may be required for functional and operational reasons to transmit information in a form that can be received and processed by the biological and psychological systems of the device's host, regardless of whether that form is naturally secure. At the same time, some devices (e.g., mnemoprostheses that are fully integrated into a natural holographic storage system of the human brain) that store and transmit information in a form that can only be processed and interpreted by the mind of the human host in whom the devices are implanted may enjoy a natural (if unconventional) form of encryption.

D. Device power and shutoff mechanisms

1. Design of device power supply and cabling

Providing an adequate and reliable power supply[97] that is protected against intentional or unintentional damage or destruction is a major challenge for the designers and operators of advanced neuroprostheses. Some devices may be able to draw on natural power sources that are present in (or can be provided through) the natural biological systems of their human host. Such 'energy harvesting' systems for implantable devices already exist. Some gather energy from sources such as body heat or the kinetic energy resulting from movement of their host's body and can often produce more than 10 milliwatts of power.[98] Other systems utilize implantable enzyme-based biofuel cells that are able to generate power from substances such as glucose and oxygen found in the host's body.[99] There are significant practical constraints on the amount of power that can be obtained from such sources.

---

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

[96] *NIST SP 800-53* (2013), p. F–193.

[97] *NIST SP 800-53* (2013), p. F–133.

[98] See Mitcheson, "Energy harvesting for human wearable and implantable bio-sensors" (2010).

[99] See Zebda et al., "Single glucose biofuel cells implanted in rats power electronic devices" (2013), and MacVitte et al., "From 'cyborg' lobsters to a pacemaker powered by implantable biofuel cells"

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Other neuroprostheses may be passive devices that rely on the activity of a host's natural neurons or other biological structures or systems to control and manipulate a device and which thus do not need their own power source. Some kinds of nanorobotic swarms may be able to draw power from chemicals found (naturally or through artificial addition) within the bloodstream of their human host. Other devices may be able to receive electricity provided wirelessly, such as through radio frequency induction.[100] Other devices may require periodic recharging through connection of a physical power cable to an external power port, permanent connection of such a cable, or the periodic replacement of a battery by means of some cover or port that is accessible either on the surface of a host's body or through an invasive surgical procedure.

2. Design of emergency shutoff mechanisms for devices and systems

For many kinds of general-purpose computers used within organizations, the recommended best practice is for a computer to include an emergency shutoff switch that can be easily accessed and used by authorized personnel, should the need arise – but which cannot be accessed or used by unauthorized parties.[101] In the case of advanced neuroprosthetic devices, a number of factors will influence whether a particular device should include a physical emergency shutoff switch and, if such a switch does exist, who will have access and authorization to use it. In some cases, the presence and use of a physical emergency shutoff switch that can shut off power to a neuroprosthetic device could cause permanent physical or psychological harm to the device's host or to others; in other situations, the presence and use of such a shutoff switch may be needed precisely in order to prevent such harm. In some cases, it is essential that the host of a neuroprosthetic device have access to such a shutoff switch (because he or she will be best positioned to know when it should be used and to physically activate it), while – insofar as possible – other persons in the host's vicinity should be prevented from knowing about the shutoff switch's existence or being able to access and use it. In other cases, the kind of emergency situations that would require immediate use of the shutoff switch would also render the device's human host physically or psychologically incapable of utilizing the switch; in these cases, the shutoff switch should be physically accessible to bystanders and other persons, and it may even be desirable to install a light or audible alarm or other system to

(2013).

[100] See Borton et al., "Implantable Wireless Cortical Recording Device for Primates" (2009).

[101] Regarding emergency shutoff methods, see *NIST SP 800-53* (2013), p. F–133.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

catch the attention of emergency medical personnel or other bystanders if the device detects a situation that calls for the use of the shutoff switch.[102]

E. Program execution protections

1. Design of protected environments for code execution

Software whose source code is unavailable to an organization or which is suspected of containing malicious code is often installed and executed by an organization only within protected and physically or virtually isolated machines running with minimal privileges.[103] For some kinds of neuroprosthetic devices whose functionality and behavioral characteristics are inherently highly influenced by or dependent on the biological structures or processes of their human host, it may not be possible to construct protected environments that fully replicate the functioning of such devices while remaining physically or virtually segregated from an actual human host. In such cases, software may need to be run within its live production environment, if it is to be run at all.

On the other hand, advanced neuroprosthetic devices may also create entirely new possibilities for constructing protected and physically or virtually isolated environments in which potentially malicious code can be run, insofar as they may allow InfoSec personnel possessing sensorimotor neuroprostheses to create and interact with information systems in a virtual environment that is separated from physical organizational systems.

2. Use of a non-modifiable operating system and applications

Designing an implantable neuroprosthetic device in such a way it loads and runs its operating system and applications from a storage medium that is permanently embedded within the device and which is hardware-enforced as read-only may be desirable,[104] insofar as it helps ensures that the device's operating system and environment will not be illicitly altered or compromised by an adversary's modification of the stored programs. However, the implications of such a practice must be carefully weighed. For example, it may sometimes occur that the operating system or applications contained on a device's read-only storage medium may need to be updated or upgraded in order to address vulnerabilities in the implanted versions of the programs that have become known. It may be difficult to implement such updates in

[102] See Chapter Three of this text for a discussion of emergency access to implanted neuroprosthetic devices and, in particular, the possible use of subcutaneous buttons.
[103] *NIST SP 800-53* (2013), p. F–227.
[104] See *NIST SP 800-53* (2013), pp. F–207-08.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

situations in which it is not legally, ethically, or practically simple for a device's operator to remove or physically access the device in order to replace or alter the storage medium after the device's implantation.

3. Planning the role of platform-independent applications

Typically, platforms are understood as "combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both."[105] The concept of a 'platform' may take on new meanings in the context of implantable neuroprosthetic devices. In some cases, the relevant 'platform' may comprise an implantable mobile computer that possesses a conventional architecture and runs a common operating system like Windows, Android, or Linux. In other cases, the 'platform' may consist of an electronic device in the form of a physical neural network comprising millions or billions of artificial neurons that are not capable of running an operating system or executing 'programs' as traditionally understood but which may nonetheless be taught to perform certain complex patterns of behavior. In other cases, the platform may include a passive device composed of biological material or electronic components that are directly guided and controlled by the activity of the cognitive and biological processes of a device's human host; in this situation, the neuroprosthetic device provides the hardware but the platform's software is found in the body or mind of its human host. This highlights the possibility that in some cases, it may not be possible to identify or understand the 'platform' created by a neuroprosthetic device simply by referring to the synthetic device itself; the platform may be constituted by or found within the larger host-device system as a whole.

It is often beneficial to utilize applications that can run on multiple platforms, insofar as this enhances application portability and the possibility of running key applications on alternate platforms, in the case of some emergency that renders their primarily platforms compromised or unavailable.[106] However, in the case of some kinds of advanced neuroprostheses, it may not only be true that applications designed for one *type* of neuroprosthetic device will be unable to run on other types of neuroprostheses, but even that applications developed for use on one neuroprosthesis implanted within a particular human being may be unable to run on other devices of the *same type* that are implanted in other human beings. Some neuroprosthetic devices may potentially store application information in biological material that incorporates the DNA of a device's human host and cannot be utilized with

[105] *NIST SP 800-53* (2013), p. F–203.
[106] *NIST SP 800-53* (2013), p. F–203.

other human hosts; other applications may be customized to interface with the unique physical structure or cognitive processes found in the natural biological neural network of a particular human host and thus will not function if run on another person's device.[107]

4. Protecting boot firmware

Some kinds of passive neuroprosthetic devices that are directly controlled by the 'operating system' provided by the biological structures and processes of their host's brain – as well as devices that include a physical neural network and whose functionality grows organically over time through learning and training – may not possess boot firmware as it is traditionally understood.[108]

5. Protections against the introduction or manipulation of binary or machine-executable code

For some kinds of neuroprosthetic devices (e.g., those utilizing a physical neural network of biomimetic synthetic neurons), certain types of biochemical or electrochemical stimuli allowed to reach a device's synthetic neurons could constitute a form of 'machine-executable code,' if the stimuli cause the neurons or their connected systems to respond by executing particular behaviors.[109]

6. Procedures for authentication of remote commands

It is especially important for a neuroprosthetic device to properly authenticate remote commands[110] in cases in which the device receives instructions from external medical control or support systems that can affect or determine the device's impact on critical health functions of its human host.

7. Controls on the execution of mobile code

By virtue of their highly customized design and structure, many neuroprosthetic devices may be incapable of using common mobile code technologies (such as JavaScript or Flash animations).[111] Nevertheless, it is important that the designers of neuroprostheses and developers of their operating sys-

[107] See the device ontologies in Chapters One and Two of Gladden (2017) for possible ways in which a neuroprosthetic device may be customized for the unique biological structures and processes – potentially as reflected in the unique psychological characteristics or knowledge – of a particular human host.

[108] See Chapter One of this text for a discussion of passive neuroprostheses of this sort. Regarding boot firmware, see *NIST SP 800-53* (2013), pp. F–226-27.

[109] Regarding binary and machine-executable code, see *NIST SP 800-53* (2013), p. F–227.

[110] *NIST SP 800-53* (2013), p. F–219.

[111] *NIST SP 800-53* (2013), p. F–198.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

tems implement adequate controls to account for the possibility that operators or hosts may attempt to install mobile code on the devices or that, for example, websites visited using a web browser or other software on a neuroprosthetic device might attempt to download and execute such code on the device.

8. Process isolation

The use of traditional practices such as hardware separation and thread isolation[112] may not be possible in the case of neuroprosthetic devices which, for example, utilize a physical neural network for storing and processing data.

F. Input controls

1. Input validation procedures

Information input validation is used to protect systems from being compromised through attacks that target the structured messages that are frequently used by an information system for communications between its different components or subsystems and which may include a combination of control information, metadata, and raw, unstructured contents.[113] If information input is not properly validated through adequate prescreening and filtering of raw input from external systems or agents, it is possible that an adversary could supply carefully designed raw input to one component of a system that would then include the raw input in a structured message sent to a different component that might erroneously interpret the raw input as though it were control information or metadata. With some kinds of sensory or cognitive neuroprostheses, for example, there may exist a theoretical possibility that simply by presenting certain carefully crafted forms and patterns of environmental stimuli in such a way that they can be absorbed as raw input by a host's sensory organs (e.g., perhaps by generating a particular series of tones that can be detected by a host's natural ears or auditory neuroprostheses, displaying certain text or symbols on a monitor viewed by the host's natural or artificial eyes, writing particular sequences of code as graffiti on the side of a building that the host will see, or uttering a particular string of words to the host in conversation), such raw input will be passed along to other components within the host's neuroprosthetic device or host-device system through a structured communication in such a way that the raw input would be interpreted as metadata or control information that will be executed or

[112] *NIST SP 800-53* (2013), pp. F–210-11.
[113] *NIST SP 800-53* (2013), p. F–229.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

otherwise utilized by the neuroprosthesis to generate some action or behavior desired by an adversary.[114]

In addition to the purely technical kind of information input validation needed to prevent such occurrences, the host or operator of a neuroprosthetic device may also potentially use such mechanisms for the prescreening and filtering of raw input (e.g., stimuli from the external environment detectable by sensory organs) to screen out particular kinds of content which the host or operator might find objectionable or undesirable on other grounds – whether for legal, ethical, cultural, or aesthetic reasons or because the blocked or limited types of content have a negative operational impact on the functionality of the device or other biological or synthetic systems or processes within its host.

2. Controls on embedded data types

In a similar fashion, controls may need to be implemented to ensure, for example, that sense data being received from the external environment by an artificial sensory organ does not contain embedded patterns of data that would be detected and interpreted by the device as (potentially malicious) executable code.[115]

3. Formulation of security policy filters

Security policy filters[116] may be implemented in order to filter, for example, the kinds of auditory sense data that are permanently recorded by an artificial ear not because the device itself is technologically incapable of recording certain kinds of information but because it should not be permanently recorded due to information security considerations.

---

[114] Hansen and Hansen discuss the hypothetical case of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights; see Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010). Although that example is of a different sort than the hypothetical cases just presented here – insofar as the case presented by Hansen and Hansen might conceivably involve a purely physical flaw or other vulnerability in the prosthetic eye that does not involve raw data being interpreted as structured data or metadata – it reflects the same basic notion that the functioning of a neuroprosthesis could be disrupted or manipulated by providing the device with certain kinds of raw data.

[115] Regarding controls on embedded data types more generally, see *NIST SP 800-53* (2013), p. F–15.

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

G. Design of a logical access control architecture

1. Planning of mandatory access controls

In some cases it may be inappropriate and potentially unethical and illegal to implement mandatory (non-discretionary) access controls[117] which, for example, prevent a device's human host from granting others access to information stored in or generated with the aid of the device. For example, imagine a neuroprosthesis that enhances its human host's powers of imagination;[118] if the end-user license agreement acknowledges that the host is the sole owner of all intellectual property (such as thoughts and ideas) that are generated with the aid of the device, the device should arguably not include controls that attempt to place mandatory limits on the user's ability to share that property with others and which block the user from utilizing his or her discretion in extending access rights to others.

2. Designing for least privilege

'Least privilege'[119] may have a unique meaning in the case of some advanced neuroprostheses whose human hosts are legally and ethically expected to possess full privileges for all aspects of a device's operation and who may determine – not during the development stage of the device but only after its implementation – how to assign privileges to other parties, subject to regular unilateral modification according to the host's wishes.

3. Isolation of access- and flow- control functions

Security functions that can (and ideally should) be segregated from the access- and flow-control enforcement functions built into a device include "auditing, intrusion detection, and anti-virus functions."[120] In the case of some neuroprostheses (such as those utilizing a physical neural network), it may not be possible to isolate such functions if they are both stored and executed holographically by components that execute many of a device's functions.

---

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

[118] For discussion of such possibilities, see Cosgrove, "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation" (2004); Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); and Gladden, "Neural Implants as Gateways to Digital-Physical Ecosystems and Posthuman Socioeconomic Interaction" (2016).

[119] *NIST SP 800-53* (2013), p. F–179.

[120] *NIST SP 800-53* (2013), p. F–185.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

H. Design of authentication mechanisms

1. Determination of actions permitted without identification or authentication

Some advanced neuroprosthetic systems (e.g., those based on a physical platform utilizing nanorobots or synthetic neurons) may not be capable of carrying out user identification or authentication; in these cases, the devices may permit and perform all possible actions without identification or authentication.[121]

2. Restriction of unencrypted embedded static authenticators

In the case of neuroprostheses that store information in the form of a physical neural network, it may not be possible to force (or even enable) the system to store its information in a form that utilizes traditional encryption methods.[122]

3. Planning of device attestation

Device attestation performs "the identification and authentication of a device based on its configuration and known operating state."[123] Some neuroprosthetic devices – such as those comprising physical neural networks[124] or biological components – may not possess stable, clearly definable configurations or operating states that can be used as the basis for device attestation. However, it may be possible to perform attestation on the basis of a cryptographic hash[125] that is stored within the device or its components, even if that information is not directly utilized by the device itself in performing its normal functions.

4. Management of user identifiers

For neuroprosthetic devices that automatically run once activated, without requiring a system logon – or which simply verify that they possess an active physical and biological interface with a human host, without determining who that host is – a device may not utilize any user or administrator accounts and thus there would not be unique account identifiers.[126] In other

[121] Regarding the InfoSec implications of actions permitted without identification or authentication, see *NIST SP 800-53* (2013), p. F–24-25.

[122] Regarding the encryption of embedded static authenticators, see *NIST SP 800-53* (2013), pp. F–97-98.

[123] *NIST SP 800-53* (2013), p. F–94.

[124] See the device ontology in Chapter One of Gladden (2017) for a discussion of such devices.

[125] *NIST SP 800-53* (2013), p. F–94.

[126] See Chapter Three of this text and its discussion of biometrics for the possibility that a neuroprosthetic device might detect whether it is situated within a living human being. Regarding identifier management, see *NIST SP 800-53* (2013), p. F–94.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

cases, the identifier for a device's human host or operator may not be an account name or string of text as commonly used but may potentially be an image, sound, electromechanical stimulus, or other kind of information that in different types of systems may generally be used for purposes of authentication rather than identification.

5. Planning authenticator management for multiple user accounts

Some implantable neuroprosthetic devices may not possess multiple 'accounts' that allow a device's operator or host to log into the system; the device may simply begin running once it is supplied with power and activated. In effect, such a device has a single account with an automatic logon. Other devices may have specialized accounts for a device's operator(s) and potentially its human host.

6. Planning of identification and authentication methods for organizational users

For neuroprosthetic devices that are acquired and operated by individual human hosts as consumer electronics devices, the robust systems for identifying and authenticating users[127] that are utilized within large institutions with dedicated IT and InfoSec personnel may not be available. On the other hand, for some kinds of neuroprostheses, a device may only physically be capable of interacting with the single human being in whose body the device is initially installed – thereby eliminating both the need and ability to create multiple user accounts or distinguish between organizational and non-organizational users.

7. Planning acceptance of third-party credentials

Allowing the use of third-party credentials to authenticate non-organizational users[128] of a neuroprosthetic device may be one approach to addressing the fact that, for example, the human host of a neuroprosthesis might experience a medical emergency when he or she is in a public place or otherwise unable to rely on specialized medical support services provided by his or her employer or healthcare provider. In such a circumstance, emergency medical responders who have no previous association with a device's host or operator may need to acquire immediate full access to the device and its functionality and an ability to override existing settings and control its operation in order to provide medical treatment and avoid harm to the host or others. It may be possible for local, national, or international governmental agencies, licensing and certification bodies, or associations of licensed medical personnel or other first responders to serve as third parties issuing credentials to individual personnel which the designers, manufacturers, and operators of advanced

[127] *NIST SP 800-53* (2013), p. F–91.
[128] *NIST SP 800-53* (2013), p. F–100.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

neuroprostheses will allow their devices to accept as authenticators – either universally, or perhaps only when a neuroprosthetic device detects that its user has entered a particular biological state or is experiencing a particular medical condition.[129]

8. Architecture for adaptive identification and authentication

Some neuroprosthetic devices may utilize adaptive identification and authentication.[130] For example, the host or operator of a motor neuroprosthesis may be able to operate an artificial limb within certain nominal physical parameters without requiring special identification, but attempting to instruct the limb to operate in a way that would create a danger of significant damage to the device or its host may trigger a request from the system for additional authentication information before the instruction is executed. Similarly, for reasons of physical or psychological safety, an artificial eye or ear might possess built-in artificial constraints in the kind or quantity of incoming information that will be allowed to reach the conscious awareness of its human host; disabling such filters that limit the brightness of visual data or loudness of auditory data might be possible only after successfully submitting additional authentication information.[131]

9. Design of single sign-on capacities

If a single human host possesses multiple implanted neuroprostheses, it may be desirable for a single system (e.g., one that has direct access to the user's cognitive activity and which can be controlled by his or her thoughts) to serve as the user's interface with the collection of devices; logging on to that single gateway device would simultaneously give the user access to the other implanted systems.[132]

10. Designing password-based authentication

For some kinds of neuroprosthetic devices that interface directly with the conscious mental processes of their human host, a host's authenticator could potentially be a particular thought or memory (or the context surrounding

[129] For a discussion of certificate schemes, see, Chapter Three of this text and, e.g., Cho & Lee (2012), and Freudenthal et al., "Practical techniques for limiting disclosure of RF-equipped medical devices" (2007). Regarding the ability of IMDs to detect a medical emergency that is being experienced by a device's human host, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), pp. 921-22.

[130] See *NIST SP 800-53* (2013), p. F–102.

[131] For a discussion of psychological, social, and cultural factors that might cause the host of an implanted device to intentionally ignore, disable, or otherwise subvert a device's security features and mechanisms – even to the extent of causing self-harm – see Denning et al. (2010).

[132] Regarding single sign-on approaches, see *NIST SP 800-53* (2013), p. F–92.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

that memory) rather than a password as understood in the traditional sense of a discrete string of characters.[133] An internal thought used as a password may take on a slightly different form each time it is expressed by its user, thus it may need to be authenticated using some statistical means (perhaps employing a neural network) rather than determining whether it precisely matches some discrete piece of information used as a reference.

11. Design of authentication methods based on hardware tokens

In the case of implantable neuroprosthetic devices, it may be possible to utilize a hardware token-based authenticator that is implanted elsewhere in the body of a neuroprosthetic device's human host.[134] While the ongoing physical proximity of the hardware token to the neuroprosthetic device does not in itself guarantee that the device is still implanted within its human host, the fact that a hardware token is no longer in physical proximity to its associated neuroprosthetic device *could* indicate either that the neuroprosthetic device has been removed from its host (and should thus automatically deactivate itself and potentially wipe stored information) or that the security of the portion of the host's body in which the token was stored has been compromised (which, in some circumstances, may also be a condition that should trigger automatic deactivation of the neuroprosthesis and the wiping of information stored within it). It is also possible that implanted neuroprosthetic devices themselves could be used as authenticators to grant their host access to other (external) information systems.

12. Biometric authentication

Traditional biometric authentication methods do not require an exact match between the biometric data presented by an individual who wishes to access a system and the stored biometric data used as an authenticator; a number of both false positives and false negatives are to be expected.[135] Because of their unique (and potentially long-term or even permanent) interface with the biological structures and processes of their human host, neuro-

[133] Elements that could be employed in such an approach are discussed, e.g., in Thorpe et al. (2005); Mizraji et al. (2009); and Gladden, "Cryptocurrency with a Conscience" (2015). Regarding password-based authentication more generally, see *NIST SP 800-53* (2013), p. F–96-97.

[134] Regarding hardware-based authentication, see *NIST SP 800-53* (2013), p. F–98. For the use of RFID implants as authenticators, see Rotter et al., "Potential Application Areas for RFID Implants" (2012). See Chapter Three of this text for a discussion of the advantages and disadvantages of using external hardware tokens to allow medical personnel emergency access to an IMD.

[135] *NIST SP 800-53* (2013), p. F–98.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

prosthetic devices may be able to utilize newly developed biometric technologies and methods that are not possible for other kinds of information systems.[136]

13. Planning of authentication feedback to users

Insofar as the process of identification and authentication might take place entirely within the cognitive processes of a neuroprosthetic device's human host, it may be possible for the device to provide full authentication feedback to the device's host (e.g., displaying the actual characters of a password that is being mentally 'typed' by the device's host, without replacing the characters with asterisks to obscure their value), without the worry that the feedback may be observed or intercepted by unauthorized parties using methods such as shoulder surfing.[137]

I. Design of session controls

1. Planning of session authenticity controls

Information systems utilize controls that protect the authenticity of sessions in order to guard against phenomena like man-in-the-middle attacks and session hijacking.[138] Some kinds of neuroprosthetic devices (such as those that possess physical neural networks and interact through ongoing synaptic communication with a human host who is also a device's operator) may not utilize sessions or other commonly employed control practices such as user accounts or authentication.

2. Restrictions on concurrent sessions

For some kinds of neuroprostheses (e.g., those that include a physical neural network that interacts directly with the memory mechanisms of their host's brain), the number of concurrent sessions[139] may be limited for technological reasons to a single session – namely, that associated with the device's human host.

3. Implementation of session lockout in response to inactivity

Automatically terminating a session after a predetermined period of inactivity[140] may be hazardous with neuroprosthetic devices whose operator and

[136] See Chapter Three of this text for a more in-depth investigation of unique possibilities for the use of biometrics with neuroprosthetic devices.
[137] See *NIST SP 800-53* (2013), p. F–99.
[138] *NIST SP 800-53* (2013), p. F–201.
[139] *NIST SP 800-53* (2013), p. F–23.
[140] *NIST SP 800-53* (2013), p. F–23.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

host expect or require that a device always be ready to provide access and service, without the delay that would be required for reauthentication.[141]

4. Design of automatic session termination procedures

Session termination[142] may be impossible to implement for some kinds of neuroprosthetic devices. A device consisting of synthetic neurons that are fully integrated into the natural biological neural network of their host's brain may in effect run a single 'session' that will last throughout the host's remaining lifetime.

J. Wireless and remote-access protections

1. Preventing information leakage resulting from stray electromagnetic emissions

A neuroprosthetic device should be protected against "the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations."[143] This may be especially difficult when multiple devices implanted within a single host form a body area network (BAN) or body sensor network (BSN) whose components communicate with one another through wireless signals; the use of components that transmit signals through bodily tissue using means that do not broadcast signals into the atmosphere may reduce that risk.

The danger of information leakage may also be relatively high in the case of a neuroprosthetic device implanted within the interior of its host's body that possesses no physical port or socket accessible on the external surface of the body and which must communicate with external diagnostic, control, or support systems utilizing wireless means.

2. Planning of remote access methods

A neuroprosthetic device implanted in a human host may need to remotely access or be accessed by systems[144] that belong, for example, to the device's manufacturer, operator, or a dedicated medical support team. Automated monitoring, encryption, and use of managed access control points may be desirable in such circumstances. Such access need not necessarily be wireless, if a neuroprosthetic device has an external port that allows for a wired connection.

---

[141] See Chapter Three of this text for a discussion of the need for 100% availability for some kinds of neuroprosthetic devices.

[142] *NIST SP 800-53* (2013), p. F–24.

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

3. Protection against wireless jamming and electromagnetic interference

A system can potentially be protected from intentional jamming through the use of unpredictable wireless spread spectrum waveforms, while other technologies may provide protection against unintentional jamming or interference (e.g., from nearby devices using the same wireless frequencies).[145] This is especially important in the case of neuroprosthetic devices whose activity can have a critical impact on the health of their human host and whose successful functioning depends on effective wireless communication with other implanted devices or external support systems.

K. Design of backup capabilities

1. Planning of alternate data processing site(s)

The use of alternate processing sites[146] for the processing of information by a neuroprosthetically augmented information system may not be possible if the act of processing is in part performed by the neurons within the host's brain or other biological systems within the host's body or if processing can only be carried out by a device when it enjoys a direct physical interface with the host's brain or body.

2. Planning of alternate data storage site(s)

The use of an alternate storage site[147] external to the body of a device's human host for storing information generated by an implanted neuroprosthetic device may not be possible for some devices that store information in particular kinds of systems (such as a physical neural network[148]) or which lack an adequate means of transmitting the relevant quantity and type of information to external systems.

3. Design of backup communications systems

A neuroprosthetic device may or may not be capable of using general-purpose communications technologies and services as a backup system if the device's own telecommunications system (which may be proprietary or demonstrate unique specifications for its speed, capacity, and format) were to fail or be disrupted.[149]

---

[145] *NIST SP 800-53* (2013), p. F–211.

[146] *NIST SP 800-53* (2013), pp. F–83-84.

[147] *NIST SP 800-53* (2013), p. F–83.

[148] See the device ontology in Chapter One of Gladden (2017) for a discussion of the structure and mechanics of such systems that include or comprise physical artificial neural networks.

[149] Regarding contingency planning for telecommunications services, see *NIST SP 800-53* (2013), p. F–85.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

4. Design of information backup methods

For some kinds of advanced neuroprostheses (such as those utilizing a complex physical neural network and holographic storage system) it may be impossible to create a coherent backup, insofar as this would require taking a 'snapshot' of the entire constantly-changing system at a single instant, but the processes available for detecting and recording the state of information within the system's components can only scan components sequentially and require a long period of time to complete a single full scan of the system.[150]

5. Planning of safe mode behavior for devices

For some kinds of neuroprosthetic devices it may be desirable to develop a safe mode[151] with a predefined and limited set of features and operations that can either be manually activated by a device's operator or human host if it becomes apparent that the host is entering (or about to enter) some situation in which unrestricted operation of the device would be hazardous to the host or others or which will be automatically activated if the device detects that certain conditions are met.[152] Note that if activating a device's safe mode will result in a loss of consciousness or in some other impairment for the device's host, then the device may also need to possess a mechanism for determining when to automatically exit safe mode and resume normal operations, insofar as the host would not be able to manually initiate such an action.

L. Component protections

1. Controls to assure component authenticity

Preventing the use of counterfeit components is especially important in the case of neuroprosthetic devices in which the discovery that counterfeit components (which may potentially be constructed from toxic materials or of otherwise substandard quality) had been used in a neuroprosthetic device

[150] Regarding related technologies that have been proposed by some transhumanists as a possible path toward brain emulation of 'mind uploading,' see Koene, "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation" (2012); Proudfoot, "Software Immortals: Science or Faith?" (2012); Pearce (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). Regarding information system backups, see *NIST SP 800-53* (2013), p. F–87.

[151] *NIST SP 800-53* (2013), p. F–89.

[152] Regarding the possibility that an IMD could discern when, e.g., a medical emergency is being experienced by its human host, see Denning et al. (2010), pp. 921-22. See Chapter Three of this text for a broader discussion of failure modes for neuroprosthetic devices during emergency situations.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

may necessitate complex, expensive, dangerous, and legally and ethically fraught surgery to extract a device and replace the components.[153]

2. Customized design for critical device components

For some kinds of neuroprosthetic devices, the in-house development of customized, nonstandard components (which may be less vulnerable to standard attacks that adversaries might be likely to employ[154]) may be a natural and even necessary aspect of a device's development. For example, in the case of neuroprostheses that utilize biological components that incorporate a host's DNA or whose security functionality depends on unique features of the host's mind (such as memories unique to that host[155]), each device may in effect be deeply customized and 'nonstandard.'

3. Designing approaches to device identity and traceability

For neuroprostheses that are housed permanently within the body of a human host and that cannot easily be physically inspected or extracted, the confirmation of identity and traceability of such devices and their components may need to be accomplished using technologies such as RFID tags[156] that can be checked wirelessly by a reader external to a host's body. In the case of some kinds of advanced neuroprostheses utilizing biological components, it may be possible to incorporate identifying marks, codes, supporting documentation, and other information into the genetic sequences of the biological material.[157]

4. Planning tamper-resistance mechanisms for the entire SDLC

The tamper-resistance mechanisms that are legally and ethically permissible and practically feasible during the pre-implantation production and testing of a neuroprosthetic device may be entirely different from those that are possible and desirable during the operations and maintenance or disposal phases of the device's SDLC.[158]

---

[153] For medical risks relating to surgery for the implantation of even 'simple' implants such as passive RFID devices, see Rotter et al., "Passive Human ICT Implants: Risks and Possible Solutions" (2012). Regarding component authenticity, see *NIST SP 800-53* (2013), p. F–180.

[154] See *NIST SP 800-53* (2013), p. F–181.

[155] See Chapter Three of this text for a discussion of the possibility of using a host's thoughts and memories as biometric access controls.

[156] Regarding identity and traceability, see *NIST SP 800-53* (2013), p. F–172.

[157] For such possibilities, see Church et al. (2012).

[158] Regarding the development of tamper-resistance mechanisms for multiple phases of the SDLC, see *NIST SP 800-53* (2013), p. F–180.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

5. Removal of unsupported system components

Typical best practices of removing and replacing system components[159] once they are no longer supported by their designer, manufacturer, or provider may be difficult or impossible to implement in the case of devices that have been implanted in a human host and whose removal would require complex, expensive, or dangerous surgical procedures or would otherwise create a possibility of physical or psychological harm for a device's host.

M. Controls on external developers and suppliers

1. OPSEC activities targeted at device or component suppliers

An organization may employ utilize operations security practices and safeguards in relation to current and potential suppliers.[160] In that context,

> OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain.[161]

As employed by some organizations, OPSEC practices and tactics may sometimes lead an organization to "withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end user, or users, of information systems, system components, or information system services."[162] Before they can be implemented, careful attention must be given to the legal and ethical implications of such OPSEC practices in the case of advanced neuroprosthetic devices. For example, a supplier that is led to believe that it is producing components for use in neuroprosthetic devices to be implanted in mice for experimental research may utilize a different level of care in producing the components (and, indeed, may make a different decision about whether to enter into a contract to supply the components) than it would have done had it been aware of the fact that its components would be incorporated into neuroprostheses to be implanted in human hosts for use in their performance of critical tasks – even if the supplier's knowledge of the true circumstances of the devices' ultimate use would not in any way have affected the specifications of the components that the client

[159] *NIST SP 800-53* (2013), p. F–182.
[160] *NIST SP 800-53* (2013), p. F–171.
[161] *NIST SP 800-53* (2013), p. F–171.
[162] *NIST SP 800-53* (2013), p. F–171.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

organization had asked the supplier to produce. Complex problems involving legal liability, moral responsibility, corporate social responsibility, and informed decision-making can arise if OPSEC activities prevent the free and robust flow of accurate information between an organization, its suppliers, and other parties involved with the development and implementation of advanced neuroprosthetic devices.

On the other hand, in situations in which the personal health information and sensitive data about the cognitive processes (including thoughts, memories, and emotions) of particular human hosts is involved, an organization may have a legal and ethical responsibility not only to conceal the detailed information that is received, stored, generated, or transmitted by the neuroprosthetic devices that it operates but even any incidental or circumstantial information that could potentially be used by suppliers to ascertain (or even guess at) the identity of a device's human host.[163] This may be especially important in cases in which a host is a significant political, business, artistic, or entertainment figure, a military or police operative, or some other individual whom unauthorized parties may have a particular interest in observing, stealing information from, blackmailing, extorting, or otherwise compromising or exploiting (i.e., through so-called '**whaling**' attacks).

2. Formulation of procedures, standards, and tools for developers

With advanced neuroprosthetic devices, it is especially important that suppliers and developers follow a well-defined and thoroughly documented development process for components and services, since in the case of unforeseen operational emergencies (such as a critical negative impact on the health of a device's human host that arises unexpectedly) it may be necessary to quickly retrace and analyze steps in the development of a component or service in order to formulate a response that can prevent serious harm to the device's host or to others.[164]

3. Security testing policies for third-party developers

Some practices that an organization may typically require of third-party software providers – such as static code analysis and manual code analysis[165]

[163] For discussions of such issues, see Kosta & Bowman (2012); McGee (2008); Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010); Hildebrandt & Anrig (2012); and Brey (2007).

[164] Regarding the creation of development processes, standards, and tools, see *NIST SP 800-53* (2013), p. F–174.

[165] *NIST SP 800-53* (2013), pp. F–166-69.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

may not be relevant or possible in cases in which, for example, neuroprosthetic devices include physical neural networks that do not execute programs or code as traditionally understood.[166]

4. Supervision of developer configuration management

Effective monitoring and supervision of developers' configuration management[167] by an organization is especially important in cases where the developer of, for example, the OS or software applications installed in implanted neuroprosthetic devices maintains direct access to the software and periodically pushes out software updates, patches, or configuration changes to devices that are implanted and in use.[168]

5. Protections for component supply chains

It is possible that adversaries may choose to identify and target an organization's supply chain of components or services needed for the design, production, implementation, maintenance, or operation of organizational information systems rather than directly targeting the information systems themselves. *NIST SP 800-53* thus notes that "Supply chain risk is part of the advanced persistent threat (APT)"[169] that organizations face. An adversary could potentially execute such an attack by compromising a supplier and covertly corrupting or manipulating the supplier's production processes, so that components produced by the supplier for an organization have been produced using improper materials that will disintegrate, break, or otherwise fail (or, in the case of an advanced neuroprosthesis, potentially poison a device's host or release other biologically or psychologically active agents into the host's body) after the information system is in use, or components may have been corrupted with malware or designed with unauthorized backdoors that will allow adversaries unauthorized access to the system after it is in use.[170] In the case of some advanced neuroprosthetic devices, the number of suppliers producing certain necessary components may (at least initially) be quite small: such a phenomenon is disadvantageous, insofar as it bars an organization

[166] For a discussion of, e.g., neuroprosthetic devices based on physical neural networks that do not execute traditional programs, see the device ontology in Chapter One of Gladden (2017).

[167] *NIST SP 800-53* (2013), pp. F–164-66.

[168] See Chapter Five of this text for a discussion of the roles and responsibilities of OS and application developers for neuroprosthetic devices.

[169] *NIST SP 800-53* (2013), p. F–170.

[170] Regarding backdoors intentionally built into implantable medical devices to allow emergency access to medical personnel – which could potentially be exploited by sufficiently knowledgeable adversaries – see Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012); Halperin et al., "Security and privacy for implantable medical devices" (2008); and Chapter Three of this text.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

from pursuing the typical approach of minimizing supply chain risk by acquiring components from multiple suppliers, although it is potentially advantageous, insofar as it allows an organization to concentrate its information security resources and efforts on securing the operations of just a single supplier or small group of suppliers.

6. Scrutiny of external information system services and providers

When engaging external information system service providers[171] in relation to advanced neuroprostheses, an organization must be careful that the external service providers do not receive access to the biological processes of devices' human hosts in a way that may be illegal or unethical; consent that has been given by the hosts for the organization to access and use information or to manipulate their internal biological or cognitive processes may or may not apply to external service providers acting on behalf of the organization. Moreover, it is not enough for an organization to satisfy itself that it does not possess conflicts of interest or other potentially harmful characteristics that could impair or call into question its ability to ensure the information security of devices' human hosts; an organization should also seek and obtain assurance that potential external service providers do not possess conflicts of interest, ulterior motives, or other traits that may give reasons for neglecting or actively compromising the information security of neuroprosthetic devices' human hosts, either as a group or in specific cases (e.g., with regard to human hosts who are significant political, military, business, or entertainment figures or otherwise likely targets of whaling attacks).

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. Environmental protections

1. Fire protection methods

Although it may not be possible to build full fire-suppression systems directly into neuroprosthetic devices, some devices that are composed of flammable materials or whose operation has the potential to generate excessive

[171] *NIST SP 800-53* (2013), pp. F–162-64.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

heat or sparks may need to at least include built-in fire-detection systems, with a device's host or operators maintaining external fire-suppression systems that are always available for use in emergencies.[172]

2. Design of temperature and humidity controls

It may be crucial to implement systems that maintain a neuroprosthetic device within a predetermined range of temperatures and which ensure that other internal and external environmental conditions are maintained – not only to ensure that the device remains within appropriate operating parameters but also that surrounding biological tissue and processes (which may be sensitive to even minute temperature changes) are not damaged by excessive heat or other emissions from the unit.[173]

3. Planning the location of information system elements

General best practices include choosing – insofar as is feasible – to house information system components in a location that is protected against "flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation" and which lacks "physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones)."[174] In the case of advanced neuroprosthetic devices, the fact that a device's human host is potentially able to take a device anywhere in the world may make it difficult or impossible to prevent the neuroprosthesis from being brought into areas exposed to such situations – a danger that is present for other types of mobile devices more generally.

4. Design of emergency power systems

For some kinds of neuroprosthetic devices, it may be possible and desirable to utilize an emergency power system[175] (such as one that requires an external power cable to be plugged into a visible external port or jack in a neuroprosthetic device) that is not practical in non-emergency situations, when a device's host expects to be able to move freely at will between different environments without the need to be plugged into a fixed power source. Small internal batteries may also be able to provide emergency power for a limited

[172] Regarding fire protection, see *NIST SP 800-53* (2013), p. F–135.

[173] Regarding temperature and humidity controls, see *NIST SP 800-53* (2013), p. F–135.

[174] *NIST SP 800-53* (2013), p. F–137.

[175] *NIST SP 800-53* (2013), p. F–134.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

period of time, even if they would be inadequate for powering a device for sufficiently long periods during everyday non-emergency use.

B. Contingency planning

1. Development of contingency plans

The development of effective contingency plans[176] for advanced neuroprosthetic devices is essential, insofar as a failure or disruption in service for some devices may instantaneously result in life-threatening harm for a device's human host or others. A contingency plan may contain procedures for continuing or resuming either all or some of a device's functions and preserving critical assets in the face of various disruptions – if not through the device itself then through other available systems.

2. Contingency training

Contingency training[177] may be especially important for a device's human host if the failure or disruption of the device's service will leave the host with only a limited window of time in which to carry out critical remedial actions before the service failure leaves the host incapacitated and unable to carry out such steps.

3. Testing of contingency plans

Some kinds of contingency plan testing (such as the use of walk-throughs and checklists)[178] may be easy to carry out; however, an accurate full-scale simulation of some kinds of contingencies may be difficult to perform insofar as it would require simulating certain kinds of mental phenomena or incapacities on the part of a human host and the impact that these would have on the host, and replicating such conditions cannot be accomplished without causing actual harm to the host.

C. Tracking of system component inventory

A neuroprosthetic system's operator should ideally keep an inventory of all devices in use that records each device's "manufacturer, device type, model, serial number, and physical location."[179] However, in the case of some neuroprosthetic devices (such as those grown or assembled from living biological material or comprising a swarm of myriad nanorobots) it may be dif-

[176] *NIST SP 800-53* (2013), p. F–78.

[177] *NIST SP 800-53* (2013), p. F–81.

[178] *NIST SP 800-53* (2013), p. F–82.

[179] *NIST SP 800-53* (2013), p. F–73.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

ficult to adequately capture the nature of a particular device using such descriptors, as each device may, in effect, be wholly unique and possess a form that is constantly shifting and evolving.[180]

D. Selection of device recipients and authorization of access

In the case of neuroprostheses operated by large institutions (e.g., devices operated by a military or intelligence agency for intelligence-gathering purposes), an organization may maintain comprehensive and detailed records of which human beings are serving as the hosts for which devices; no other human beings are authorized to serve as the hosts for those devices, and the list of other individuals (e.g., organizational medical personnel) who are authorized to gain physical access to the devices is limited. On the other hand, with neuroprosthetic devices that are sold to the public through retail outlets as consumer electronics devices, there may be no reliable centralized record of which devices are implanted in which human beings and who is a device's 'authorized' operator.[181]

E. Physical hardening of the host-device system and supersystem

1. Restrictions on the use of portable media

For computers that are permanently physically located within a secured and supervised facility belonging to an organization, it may be possible for the organization to create and enforce administrative, logical, and physical controls (such as metal cages surrounding the computers[182]) that block users from utilizing ports or slots on the computers to insert portable storage media such as flash memory cards. In the case of neuroprosthetic devices implanted in human beings who are free to travel wherever they want and who may enter diverse kinds of environments and situations, it may not be possible to implement controls that will always reliably prevent portable storage media from being inserted into a neuroprosthetic device's slots and ports; if preventing the unauthorized use of portable storage media is a top priority, it may be necessary for the device's designer and manufacturer to construct the device in such a way that no such ports or connections are present and any effort to add them by an unauthorized user would disable the device.[183]

[180] Such a possibility would raise challenges for use of the device ontology presented in Chapter One of Gladden (2017): in that case, the ontology would become a way of specifying a device's general structural and operational parameters rather than its exact current characteristics.

[181] Regarding physical access authorizations, see *NIST SP 800-53* (2013), pp. F–127-28.

[182] *NIST SP 800-53* (2013), p. F–124.

[183] See the device ontology in Chapter One of Gladden (2017) for different aspects of a neuroprosthetic device's physical structure and accessibility, including the presence or absence of physical input and output mechanisms.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

2. Controls on access to ports and I/O mechanisms

For implantable neuroprosthetic devices which, for some reason, are required to include physical connection ports (e.g., USB or specialized proprietary ports) or input/output devices (such as microSD card readers or specialized proprietary memory chip readers) that are accessible from the exterior of their host's body, it may be desirable from the perspective of information security to disable such I/O devices at all times except for occasions when they are enabled through an explicit command from the operator of a neuroprosthesis or occasions when a medical emergency experienced by a neuroprosthetic device's host causes the ports and I/O devices to be automatically enabled in order to allow for the delivery of medical treatment by emergency personnel.[184]

Note that the legal, ethical, and practical implications of such design decisions must be carefully considered: for example, if it is commonly known that a neuroprosthetic device's exterior connection ports and I/O devices will be automatically enabled in the case of particular kinds of medical emergencies experienced by the device's human host, an adversary could potentially purposefully induce a relevant kind of medical emergency for the device's host (e.g., through a physical, biological, or chemical attack or intervention) in order to gain access to fully enabled connection ports or I/O devices that the adversary can use to compromise the neuroprosthetic device.

3. Limitations on implants' wireless transmission levels for InfoSec- and safety-related reasons

Limiting the power levels of wireless transmissions[185] from a mobile device or utilizing directional antennas is a useful practice for reasons of ensuring information security; in the case of some implantable neuroprosthetic devices it may also be desirable to help ensure the long-term health and safety of a device's host and avoid undesirable interference with other implanted systems.[186]

4. Use of lockable casings for devices

Depending on the nature of a neuroprosthetic device, it may be necessary to ensure that legitimate, licensed emergency personnel have a way to unlock

[184] See Chapter Three of this text for a discussion of allowing special access to neuroprosthetic devices during health emergencies that affect their human host. Regarding access to ports and I/O devices, see *NIST SP 800-53* (2013), p. F–212.

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

[186] See Chapter Three of this text for a discussion of the reliance on wireless communication with external systems that is characteristic of many kinds of implantable neuroprosthetic devices.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

or bypass lockable casings[187] in order to physically access a device when providing emergency medical treatment to its human host.[188]

F. Logical hardening of the host-device system and supersystem

1. Verification of transmission source and destination points

Even when a neuroprosthetic device is intended solely to transmit information between different systems that are permanently embedded within the body of its human host and not to the external environment, controls may need to be implemented to ensure that the origin and destination points of such communications are indeed the intended systems.[189]

2. Prevention of electronic discovery of devices or components

Neuroprosthetic devices that consist largely or entirely of biological material may possess a natural ability to prevent their detection as information systems (or components of such systems) by sensors or other detection mechanisms that are designed to identify, locate, and analyze conventional electronic information systems.[190]

3. Restrictions on wireless transmission strength to reduce detection potential

Even if adversaries are unable to decipher the contents of messages that are being wirelessly transmitted by a particular device, simply being able to detect the existence of the device and the fact that it is transmitting signals and to potentially pinpoint its geospatial location provides an adversary with useful information. Reducing the strength of wireless transmissions from an implanted neuroprosthetic device may reduce its detectability.[191] Some kinds of implantable neuroprosthetic devices may already be restricted to utilizing low-power transmissions in order to avoid causing potential harm or disruptive side-effects for biological systems and material within their host's body (e.g., heat generated by the absorption of radio frequency radiation).[192] At the same time, transmission signal strengths must be sufficient to ensure that

[187] Regarding such casings, see *NIST SP 800-53* (2013), p. F–129.

[188] For a discussion of emergency access to implantable neuroprosthetic devices, see Chapter Three of this text as well as Clark & Fu (2012); Rotter & Gasson, "Implantable Medical Devices: Privacy and Security Concerns" (2012); and Halperin et al. (2008).

[189] Regarding the related concept of domain verification, see *NIST SP 800-53* (2013), p. F–17.

[190] Regarding methods to prevent the electronic discovery of devices or components, see *NIST SP 800-53* (2013), p. F–191.

[191] Regarding methods for reducing the potential detection of wireless transmissions or devices, see *NIST SP 800-53* (2013), p. F–211.

[192] See Zamanian & Hardiman, "Electromagnetic radiation and human health: A review of sources and effects" (2005).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

physical or psychological harm does not result for a device's host due to a device's failure to execute successful wireless communications with other implanted devices or external medical support or control systems.

4. Signal parameter identification to detect deceptive communications

Some information systems may utilize 'radio fingerprinting techniques' to identify and track particular devices according to the signal parameters displayed by their wireless transmissions; conversely, other devices may attempt to elicit communications from or manipulate communications with a system by intentionally imitating the signal parameters of a particular device that is already trusted by the system.[193] Utilizing appropriate techniques (such as anti-fingerprinting mechanisms employing unpredictable signal parameters) to counter such possibilities is especially important in the case of neuroprosthetic devices whose only means of communication with necessary external support and control systems is through wireless transmissions.[194]

5. Protections against spam

For individuals possessing advanced neuroprostheses that edit or replace their natural sensory input to create an experience of augmented or virtual reality,[195] spam might come in the form of messages, advertisements, alerts, or any other kind of virtual audiovisual or other sensory phenomena designed to elicit some behavior from a neuroprosthetic device's host. For individuals possessing some kinds of advanced cognitive neuroprostheses, spam may potentially even take the form of memories, emotions, desires, beliefs, or other mental phenomena that are directly inserted into or created or altered within a host's cognitive processes by some external agent.[196]

Some kinds of neuroprosthetic devices may be able to utilize spam protection mechanisms that learn what is spam by directly detecting the physical or psychological reaction presented by a device's human host to incoming messages and stimuli, thereby supplementing or enhancing traditional learning mechanisms such as Bayesian filters that are often employed in spam protection systems.[197]

---

[193] *NIST SP 800-53* (2013), p. F–212.

[194] See Chapter Three of this text for a discussion of the reliance on wireless communications that is found with many kinds of implantable neuroprosthetic devices.

[195] For the possibility that a device that has been designed to receive raw data from the external environment could have that data supplemented or replaced by other data transmitted from some external information system (which could create new opportunities for the delivery of spam content), see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012).

[196] Regarding protections against spam, see *NIST SP 800-53* (2013), p. F–228.

[197] Regarding anti-spam systems utilizing a continuous learning capability, see *NIST SP 800-53*

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

6. Protections against data mining

Some kinds of neuroprosthetic devices (such as those that utilize physical neural networks and holographic storage mechanisms) may inherently possess robust protections against many typical data-mining technologies or techniques.[198]

G. Device initialization and configuration controls

1. Specification of baseline configurations

It may be difficult or impossible to specify a baseline configuration[199] for some kinds of advanced neuroprostheses, such as a mnemocybernetic device consisting of a physical artificial neural network that is integrated at the synaptic level with natural neurons in the host's brain and which does not have a set of discrete settings that can be centrally updated and applied to all individual neurons throughout the system after it has been activated. It may be impossible to intentionally roll back such a device to a previous configuration (or even to identify what such a configuration might be).

2. Automatic configuration changes

Some neuroprosthetic devices may possess a configuration that is continuously altered in automatic response to stimulation and other activity by the host's biological systems with which a device is integrated, without any means for its operator to directly control the configuration changes.[200]

3. Analysis of the InfoSec impact of configuration changes

For some neuroprosthetic devices it may not be possible to fully analyze the security impact of potential configuration changes prior to actually implementing them, if a device's exact response to the changes depends on the precise action of psychological or biological processes within the device's human host that cannot be simulated in a virtual test environment.[201]

4. Dangers of design for least functionality

In the case of a neuroprosthesis that is designed primarily to provide some necessary medical service or functional enhancement to its human host rather than to secure particular information, there may be non-security reasons

(2013), p. F–228.

[198] Regarding data mining protections, see *NIST SP 800-53* (2013), p. F–35.

[199] *NIST SP 800-53* (2013), p. F–64.

[200] Regarding configuration change control, see *NIST SP 800-53* (2013), p. F–66.

[201] Regarding analyses of the security impact of configuration changes, see *NIST SP 800-53* (2013), p. F–68.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

for the device to offer the greatest functionality possible rather than the least allowable.[202]

5. Non-privileged access for non-security-related device functions

With some kinds of neuroprosthetic devices, it may be a technological and functional necessity for a device's operator or host to possess privileged access to the system, even when it is being used to perform non-security-related functions.[203]

6. Software usage restrictions

Software restrictions are often implemented to ensure that software is used in accordance with its licensing restrictions and to ensure that software such as a peer-to-peer file-sharing program is not used "for the unauthorized distribution, display, performance, or reproduction of copyrighted work."[204] In the case of neuroprosthetically augmented information systems, operators must be careful to ensure – for legal and ethical reasons – that any software restrictions that are capable of disabling or constraining the use of software products do not do so at a time or in a manner that could cause harm to a device's human host or others.

The policing of peer-to-peer file-sharing will also be complicated by the fact that in effect, the mind of a device's human host is a 'peer-to-peer file-sharing program' that is frequently exchanging information of all kinds with other human beings. Complex legal questions may also arise surrounding what constitutes a 'display or performance' of copyrighted material: for example, in the past, using a hidden video camera to videotape a movie that was being shown in a commercial cinema and then uploading the bootleg video to a video-streaming website would have been considered an illicit use of copyrighted material, but observing the film carefully with one's natural eyes, storing that sensory record in one's natural memory systems, and later using one's voice to describe the film to one's friends would not have been considered an illicit act. Such boundaries between licit and illicit usage may become blurred, for example, if one possesses artificial eyes or a mnemoprosthetic device that allow one to record *all* of one's daily visual experience – and not simply a film in a cinema – with high resolution and perfect fidelity or if one possesses an artificial voice-box that allows one not simply to speak with

[202] See Chapter Three of this text for a discussion of the trade-offs that sometimes occur between increased information security and increased functionality for neuroprosthetic devices. Regarding design for least functionality, see *NIST SP 800-53* (2013), pp. F–71-73.
[203] Regarding non-privileged access for non-security-related device functions, see *NIST SP 800-53* (2013), p. F–19.
[204] *NIST SP 800-53* (2013), p. F–76.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

one's 'own' natural voice but to play back any recorded sounds, including those that one may have overheard during a film screening.[205]

Complex questions that must be resolved by law, regulation, or individual licensing agreements will also arise regarding intellectual property that is created with the aid or participation of a neuroprosthetic device. If a human host utilizes a device that enhances his or her memory, imagination, or artistic, mathematical, physical, or reasoning abilities, then any literary or artistic works, performances, inventions, or discoveries developed by the host may ultimately be the property of the neuroprosthetic device's manufacturer, provider, app developer, operator, or human host, or it may be owned jointly by some combination of parties.

7. Restrictions on the installation of software by users

Blocking the installation of software on a neuroprosthetic device by its user may or may not be legally and ethically permissible, as in some situations this may be equivalent to blocking a human being from adding thoughts, memories, or other permissible content to his or her own mind.[206]

8. Restrictions on device use

An organization may wish to prohibit or restrict the use of devices[207] that possess environmental sensing or recording capabilities (such as smartphones or cameras) within particularly sensitive facilities or areas. It is one matter for an organization to deny entry to its facility to individuals possessing handheld cameras (or to require that such individuals temporarily deposit their cameras for safekeeping with the organization's personnel upon entering the facility); it is another matter to deny entry to individuals who possess certain kinds of implantable neuroprosthetic devices, such as artificial eyes that possess the same functionality as handheld cameras. In the latter case, such neuroprostheses may, from a legal and ethical perspective, be treated as implantable medical devices, and an organization's refusal of entry or service to a person possessing such a device may in some cases be considered an unlawful form of discrimination on the basis of the person's health or medical status. Even conducting the kind of searches that may be required in order to determine the presence of some kinds of implantable neuroprosthetic devices in visitors to an organizational facility (e.g., potential custom-

[205] For the notion that a neuroprosthetic device could be used for sensory recording or playback, see Merkel et al. (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee (2008), p. 217.

[206] Regarding conventional controls on user-installed software, see *NIST SP 800-53* (2013), p. F–76-77.

[207] *NIST SP 800-53* (2013), p. F–213.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

ers visiting a company's retail store or showroom) may be considered an impermissibly intrusive procedure that illicitly gathers information about visitors' personal medical history and status without their express consent. Efforts by an organization to proactively jam or obstruct the functioning of some kinds of neuroprosthetic devices (such as attempts by a theater owner to prevent the use of artificial eyes to record a performance) would likely encounter legal, ethical, and practical obstacles similar to those encountered by organizations that have sought to jam the functioning of smartphones on their premises.[208]

9. Restrictions on the use of sensors and access to sensor data

An organization's ability to restrict the activation and use of environmental sensors (such as cameras, microphones, accelerometers, GPS systems, temperature gauges, and other mechanisms) in devices belonging to the organization is a critical element of information security.[209]

In the case of sensory neuroprostheses such as artificial eyes, an organization must often make a device's environmental sensing capabilities available to a device's host and operator at all times – with no delays, distortions, or other failures in service – while at the same time blocking all unauthorized parties from accessing (or potentially even knowing about the existence of) the device's sensor capacities. Adversaries who gain unauthorized access to a neuroprosthetic device's sensor capabilities could potentially use that ability to conduct covert and illicit surveillance on the device's human host, the organization by whom the host is employed, other organizations or individuals with whom the host is associated, or even organizations or individuals who have no direct connection with the host but whom the host happens to be passing by at the moment. In the case of cognitive neuroprostheses, a device itself may not possess direct access to raw sense data from the environment, but it may be able to indirectly access such data through its host's memory or other cognitive processes. Motor neuroprostheses that are used, for example, to control the movement of an artificial limb may contain accelerometers or other sensors that are intended to gather data about the position and activity of the limb but which can be utilized by adversaries to gather information about the broader physical environment, instead.

---

[208] Regarding the technological, legal, and ethical aspects of using jamming devices to block cell phone signals in places such as movie theaters and schools, see Koebler, "FCC Cracks Down on Cell Phone 'Jammers': The FCC says illegal devices that block cell phone signals could pose security risk" (2012), and Overman, "Jamming Employee Phones Illegal" (2014).

[209] *NIST SP 800-53* (2013), p. F–213.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

10. Restrictions on device use outside of organizational contexts

Although it may be legally and ethically permissible and practically feasible for an organization to restrict the ability of its members to utilize technologies such as cameras, smartphones, printers, and scanners while in the workplace,[210] an organization's ability to restrict the use of such technologies by its employees during their personal, non-work time and away from workplace facilities is limited. This causes challenges for information security, insofar as the same sensitive, work-related information that was captured, generated, stored, or transmitted by neuroprosthetic devices during working hours in the workplace may also be present in or recoverable from the devices when their human hosts are away from the workplace and engaging in purely private activities.

H. Account management

1. Automatic removal of temporary and emergency accounts

Implementing the automatic deletion of emergency accounts after a predetermined time[211] (rather than through manual action of a device's operator) may create a potential danger to the health and safety of a device's host, if an emergency account were being used to access the device in order to perform an urgent repair or provide some emergency medical service.

2. Automatic inactivity logouts

Implementing an automatic logout after a predetermined period of inactivity[212] should be done only after careful consideration, given the fact that a device's operator or host may expect and sometimes require instantaneous access to the device's functionality, and the delay caused by a need to log into an account would be unacceptable and potentially hazardous.

3. Disabling of accounts for high-risk users

Even if the operator or human host of a neuroprosthetic device has been clearly identified as a 'high-risk individual' who is likely to use the device for unauthorized purposes or to be targeted in whaling attacks, the decision of whether to disable the individual's account may raise serious legal and ethical questions, if disabling the account could impair (or even wholly terminate) the functioning of the device, thereby causing physical or psychological harm to the device's host or to others who would in some way be affected.[213]

---

[210] *NIST SP 800-53* (2013), p. F–214.
[211] *NIST SP 800-53* (2013), p. F–9.
[212] *NIST SP 800-53* (2013), p. F–9.
[213] Regarding the disabling of accounts for high-risk individuals, see *NIST SP 800-53* (2013), p. F–

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

4. Restrictions on privileges for non-organizational users

Fully blocking non-organizational users from exercising privileged access[214] to a neuroprosthetic system may not be possible if the system must possess mechanisms allowing privileged access (e.g., by medical personnel) in the case of a medical emergency affecting a device's human host.[215]

I. Security awareness training

Security awareness training[216] is important not only for the hosts or operators of neuroprosthetic devices but also for all individuals who live, work, or otherwise spend time in environments in which it is possible that other persons may possess neuroprosthetic systems that would allow them to compromise the individuals' information security.

J. Analyzing vulnerabilities in the deployed production context

1. Attack surface reviews

An organization may conduct attack surface reviews to identify physically or electronically exposed elements of an information system that increase its vulnerability to attacks; such attack surfaces include "any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities."[217] In the case of advanced neuroprostheses, attack surfaces may comprise not only the hardware and software components of a device itself but also anatomical structures, biological systems, and cognitive processes within a device's human host.

2. Penetration testing

The traditional conceptualization of penetration testing[218] as either black-, gray-, or white-box testing takes on new aspects in the case of advanced neuroprosthetics. In a sense, it may be impossible for any developer (or outside assessor acting on behalf of the developer) playing the role of an adversary to conduct full white-box testing, insofar as that would entail being given all available schematics, documentation, and information relating to the functioning of the system – and in the case of an advanced neuroprosthetic

10.

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

[215] See Chapter Three of this text for an in-depth discussion of issues relating to emergency access to neuroprosthetic devices for medical personnel.

[216] *NIST SP 800-5* (2013), p. F–37.

[217] *NIST SP 800-53* (2013), p. F–168. See Chapter Two of this text for a discussion of vulnerabilities of neuroprosthetic devices. For vulnerabilities in IMDs generally, see Hansen & Hansen (2010).

[218] *NIST SP 800-53* (2013), p. F–168.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

device, some such information and resources may be stored in the mind of the device's host in a way that cannot be conveyed to any other party; in such a situation, only a device's human host could (if sufficiently skilled) perform true white-box penetration testing.

3. Penetration testing by independent agents

Allowing penetration testing by independent agents or teams[219] may create special dangers, insofar as independent agents who lack full access to information about the nature of a neuroprosthetic device and its human host may inadvertently employ penetration technologies or techniques that are especially likely to cause harm to that host. On the other hand, independent agents are free from conflicts of interest that may arise with penetration testing conducted by an organization's internal personnel.

4. Red team exercises

The potential use of penetration testing to identify vulnerabilities or test the resistance of an advanced neuroprosthetic device in use within a human host to hostile cyberattacks, social engineering, espionage, and other efforts at compromising information security must be carefully considered, given the possibility that such testing[220] (whether or not it is successful in exploiting vulnerabilities) may cause physical or psychological harm to the device's host or others. Legal and ethical questions arise surrounding the extent to which penetration testing may be conducted on a neuroprosthetic device that has already been implanted in a human host; however, in some cases it may be impossible to accurately simulate the performance of an implantable device outside of the unique circumstances of its implantation within its particular host. Moreover, if vulnerabilities indeed exist, penetration testing may allow them to be discovered by the neuroprosthetic device's operator and addressed before they can be exploited by hostile outside parties who might intentionally exploit them to inflict maximum possible damage to the device's human host.

5. Penetration testing of physical facilities

In the case of advanced neuroprosthetic devices, it may or may not be permissible for a device's operator to conduct penetration testing that involves "unannounced attempts to bypass or circumvent security controls associated with physical access points,"[221] if such operations create a risk that physical or psychological harm may result to a device's human host or others.

---

[219] *NIST SP 800-53* (2013), p. F–62.

[220] Regarding red team exercises, see *NIST SP 800-53* (2013), p. F–62.

[221] *NIST SP 800-53* (2013), p. F–130.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

6. Active testing of devices' response to known malicious code

A neuroprosthetic device's mechanisms for protecting the device and host-device system against malicious code can be tested "by introducing a known benign, non-spreading test case into the information system."[222] Great care should be taken and all legal, ethical, and practical implications considered before intentionally introducing such code into a neuroprosthetic device that is already integrated into the neural circuitry of a human host, as code that had previously been believed to be "benign" and "non-spreading" when studied in a laboratory setting may behave in unpredictable ways when exposed to or affected by the unique biological structures or activity of a particular human host.

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. Operations security (OPSEC)

1. Intentional misdirection to conceal information systems and their characteristics

An organization may utilize practices such as virtualization techniques, the intentional promulgation of believable but misleading information about the organization's systems or operations, the concealment of system components, and **deception nets** (including **honeynets** that intentionally utilize outdated or poorly configured software) in order to confuse adversaries and potentially lead them to undertake attacks that will be ineffective.[223] In the case of advanced neuroprosthetic devices, mechanisms designed for concealment and misdirection may need to be able to distinguish, for example, between an adversary who is attempting to break into and take control of a device for malicious purposes and emergency medical personnel who are attempting to 'break into' and take control of a device in order to save its host from some

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

[223] *NIST SP 800-53* (2013), pp. F–205-06.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247. Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

life-threatening medical danger. In the latter case, mechanisms for concealment or misdirection purposefully added to a device or its software by their developers could potentially result in financial liability and legal and moral responsibility for the developers in the case of physical or psychological harm that is caused to the device's host or others as a result of emergency responders being actively slowed or misdirected by such mechanisms.[224]

2. Concealment and randomization of communications

An adversary who is unable to gain access to the exact contents of communications may nonetheless obtain valuable intelligence by being able to observe phenomena such as the "frequency, periods, amount, and predictability" of communications.[225] Mechanisms or practices that conceal or obscure such patterns can contribute to the information security of a neuroprosthetic device; however, the ability to randomize or conceal such communications may be limited by practical functional considerations such as the need to communicate effectively with the biological systems of a device's host and the fact that many forms of communication typically utilized by a human being – and thus a host-device system (such as speech, paralanguage, and gestures) – are effective precisely because they release information into an external environment in a way that is not concealed or obscured.

3. Controlling physical access to devices outside of the organizational environment

Maintaining physical access control[226] is a challenge in the case of advanced neuroprosthetic devices. The fact that a device is implanted within the body of a human host creates a practical, legal, and ethical obstacle that may prevent casual attempts by unauthorized parties to access the device: a neuroprosthetic unit that is implanted deep within a host's brain and possesses no external physical access ports is more difficult to physically access than a computer sitting on a desktop in an exposed workplace environment.[227] On the other hand, the fact that a neuroprosthetic device is implanted in a human host who can conceivably take it anywhere in the world – and who could potentially be abducted and forcibly restrained or transported – increases the opportunity to gain physical access to the device for

[224] See Chapter Three of this text for some proposed approaches to shielding or jamming technologies that mask or conceal a neuroprosthetic device's existence but which can be disabled by emergency medical personnel when necessary.

[225] Regarding such threats and the approaches to communication concealment and randomization that can be employed to counteract them, see *NIST SP 800-53* (2013), p. F–194.

[226] *NIST SP 800-53* (2013), pp. F–128-29.

[227] See the device ontologies in Chapters One and Two of Gladden (2017) for ways in which the information security of a neuroprosthetic device can be affected by the device's physical structure and its location within or in relation to its host's body.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

unauthorized parties that have sufficient means and motivation, especially if a device possesses visible and easily accessible external slots, ports, or other physical access points. This places greater demands on an organization's OPSEC personnel to protect such devices and their hosts.

B. Control of device connections

1. Protections against unauthorized physical connections

In the case of advanced neuroprosthetic devices, unauthorized physical connections with a device[228] (or its larger host-device system) might come not only through the connection of unauthorized external electronic devices to electronic components of the neuroprosthetic device but also through the presence of biological or biochemical agents and vectors (such as viruses, microorganisms, nootropic drugs, or other chemicals or substances) that can enter a host's organism and interface with his or her biological systems.[229]

2. Automatic termination of network connections

The automatic termination of a neuroprosthetic device's network connection after an arbitrary predetermined period of time could potentially result in physical or psychological harm to the device's host or user if the termination occurred during the midst of some critical activity.[230] Some naturally occurring biological cycles that are present within the biological systems and processes of a device's host (e.g., sleep cycles or cycles of neuronal firing) may provide opportunities for the safe deallocating and reallocating of address/port pairings, the disconnecting and reconnecting of network services, or other kinds of regular processes needed for maintaining a device's security and functionality.

C. Media protections

1. Controls on access to storage media

It may be impractical, unethical, and illegal for an organization – in its effort to control access to storage media[231] – to attempt to dictate, for example, that information system media remain within the organization's secured facility when the media are contained within neuroprosthetic devices implanted in the bodies of human hosts; it may not be possible to control the

[228] Regarding protections against unauthorized physical connections, see *NIST SP 800-53* (2013), p. F–191.

[229] Neuroprosthetic devices that include biological components may be especially liable to such attacks. For the possibility of neuroprosthetic devices involving biological components, see Merkel et al. (2007); Rutten et al. (2007); and Stieglitz (2007).

[230] Regarding automated network disconnection, see *NIST SP 800-53* (2013), p. F–194.

[231] *NIST SP 800-53* (2013), pp. F–119-21.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

location of a storage medium without controlling (whether legally or unlawfully) the location of the human being in whom it is situated. If the information contained within a neuroprosthetic device is sufficiently valuable, an organization may not be able to assume that adversaries will not threaten, physically restrain, abduct, or harm the human host in whom the information's storage medium is housed in order to gain access to it.

2. Restrictions on media transport

It may be difficult or impossible to document or restrict the transporting of storage media[232] if they are contained in neuroprosthetic devices implanted in human hosts whose movements cannot legally or ethically be constrained or precisely tracked.

3. Implications of access for portable storage media

Some neuroprosthetic devices that possess an external port, media slot, or socket may allow data to be easily copied to or from portable storage media or devices, with significant implications for information security.[233]

D. Exfiltration and other output protections

1. Access controls for output mechanisms

Some neuroprosthetic devices not only include (or are connected to) traditional output devices such as radio transmitters or monitors; they are also linked to 'output devices' such as the voice-box, facial muscles, hands, and other motor organs of their human host, which can be used to produce output in the form of speech, facial expressions, hand gestures, or typed or written communication.[234] Attempting to limit a host's use of such output systems may not be legally or ethically appropriate.[235]

2. Filtering of device output

In the case of advanced motor neuroprosthetics, filtering[236] may be used to (perhaps only temporarily) prevent the execution or expression of motor behavior that is identified as being anomalous and inconsistent with the kinds of motor behaviors expected from a device and its host-device system

[232] *NIST SP 800-53* (2013), p. F–121.

[233] See the device ontology in Chapter One of Gladden (2017) for a discussion of such components of neuroprosthetic devices. Regarding portable storage devices, see *NIST SP 800-53* (2013), p. F–33.

[234] See the device ontology in Chapter One of Gladden (2017) for a discussion of different output mechanisms for neuroprosthetic devices.

[235] Regarding access controls for output devices, see *NIST SP 800-53* (2013), pp. F–130-31.

[236] Regarding information output filtering, see *NIST SP 800-53* (2013), p. F–232.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

in some given circumstances. This could potentially prevent a motor neuroprosthesis from being hijacked by an adversary and used to perform an action that might disclose sensitive information or cause physical or psychological harm, embarrassment, or other negative impacts for the device's human host, operator, or others.[237] At the same time, care must be taken that such filters do not prevent a device's host or operator from expressing legally and ethically permissible motor actions that are fully intended by the host or operator simply because they are unusual and determined by the automated filter to be anomalous or suspicious.

3. Prevention of unauthorized exfiltration of information

The unauthorized **exfiltration** of information from a neuroprosthetic device or host-device system can potentially be detected and prevented through practices such as monitoring a device's communications to detect **beaconing** from within the device (e.g., directed at an external command-and-control server from which the compromised device is awaiting instructions), analyzing outgoing communications to detect **steganography**, and using traffic profile analysis to detect other anomalous communications that may potentially indicate exfiltration.[238] In the case of neuroprosthetic devices that control or support the cognitive processes or motor activity of their human host, care must be taken to ensure that mechanisms designed to prevent unauthorized exfiltration do not slow, block, or otherwise impede a host's communications and interaction with the external environment in a way that could result in physical or psychological harm to the host or others. In some circumstances, it may not be legally or ethically permissible to immediately block outgoing communications – even if an occurrence of ongoing unauthorized exfiltration has been confirmed – if impeding the outgoing communications could have sufficiently negative consequences for the survival or health of the device's host.

4. Mechanisms for the controlled release of information

It may be difficult or impossible to prevent the release of information[239] beyond the boundaries of a neuroprosthetically augmented information system if the mind of a neuroprosthetic device's human host is a part of that system, as the mind can express and convey information through speech, gestures, and other means that are not readily controlled.

---

[237] For the possibility of a neuroprosthetic limb being hacked by an adversary in order to manipulate its motor activity, see Denning et al. (2009).

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

E. Maintenance

1. Controls on the timing and location of maintenance activities

Conducting maintenance procedures on an advanced neuroprosthesis may require performing a surgical operation on the device's host, which would necessitate close coordination with the host and medical personnel. Even in cases when no surgical procedures are required, maintenance operations should be planned and scheduled in such a way that they do not cause undue interruption or impairment to a host's cognitive and physical capacities and, in particular, that they do not cause physical or psychological harm to the host or others. Conducting all maintenance within a secure facility may be desirable in order to ensure, for example, that automated maintenance instructions that are sent remotely to a neuroprosthetic device and which will result in a temporary device outage or change in the unit's functionality do not arrive when the device's host is engaged in performing a critical or potentially dangerous task.[240]

2. Control of maintenance equipment and software

Standard practices which prevent the unauthorized removal of system maintenance software or tools from a device and which restrict their use[241] may not be appropriate for neuroprosthetic devices that are a part of their host's organism; legal and ethical considerations may dictate that the host have full access to maintenance tools, including the ability to remove them. Emergency medical personnel treating the host may also need immediate unfettered access to some system maintenance tools that will allow them to affect or control the device's current operations, even if they are not provided full (or even partial) access to information stored within the device.[242]

3. Oversight of maintenance personnel

Efforts by a neuroprosthetic device's operator to limit who is allowed to conduct maintenance activities on the device – thereby restricting its host's ability to select his or her own maintenance personnel – may not be legal or ethical, given the device's status as an implantable device that may be considered an integral part of the host's body.[243]

Given the extremely large financial commitment that may be involved with acquiring authorized replacement parts and maintenance services for

[240] Regarding different possible service outage or maintenance schedules and their impact on a neuroprosthetic device's availability, see Chapter Three of this text. Regarding controls on the timing and location of maintenance procedures, see *NIST SP 800-53* (2013), p. F–112.

[241] *NIST SP 800-53* (2013), pp. F–113-14.

[242] See Chapter Three of this text for a discussion of different approaches to providing medical personnel with emergency access to a neuroprosthetic device.

[243] Regarding the control of maintenance personnel, see *NIST SP 800-53* (2013), p. F–116.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

some kinds of neuroprosthetic devices, there may be strong financial incentives for the human hosts (or potentially operators) of such devices to seek out replacement components and services through less expensive unauthorized black- or gray-market channels offering pirated or counterfeit components and services that lack quality guarantees or warranties and are provided by individuals lacking formal training, licensing, or insurance. Such unauthorized channels may sometimes offer products that are more expensive than their authorized counterparts because they are free from standard security or DRM mechanisms or have been legally banned or offer services that cannot legally be provided or received.[244]

4. Predictive maintenance

Efforts to require the host of a neuroprosthetic device to submit to mandatory preventative device maintenance on the basis of predictive algorithms, a fixed calendar, or an *ad hoc* decision on the part of the device's operator may or may not be legal, if the maintenance may impact the host's cognitive or physical functioning and he or she does not wish to submit to it.[245]

5. Prevention of predictable failures

A best practice is to determine the mean time to failure (MTTF) for information system components not simply by relying on reported industry averages but by calculating the MTTF for components as they are used in particular installations by an organization.[246] Knowing the MTTF for components in use helps the organization to ensure that it has an adequate supply of replacement components on hand and is ready to repair or replace components when needed.

For some kinds of neuroprosthetic devices, the MTTF for individual components or a device as a whole may be influenced or determined by factors relating to the unique biological structures or processes of the device's individual human host. In such cases, it may be impossible to accurately estimate the MTTF for components in a particular device until the device has been put into operation and components have begun to fail.

---

[244] For the possibility of hosts modifying their own devices in unanticipated and potentially unwise and illicit ways, see Denning et al. (2010).

[245] For a discussion of predictive maintenance, see *NIST SP 800-53* (2013), p. F–118.

[246] Regarding predictable failure prevention, see *NIST SP 800-53* (2013), p. F–231. See Chapter Three of this text for a discussion of mean time to failure, mean time to repair, and availability for advanced neuroprosthetic devices.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

F. Transmission of security alerts, advisories, and instructions

In the case of some kinds of sensory or cognitive neuroprostheses, it may be possible for an organization to deliver a security alert or directive[247] instantaneously and directly to the conscious awareness of a device's host through sensory input or augmented reality. However, if such methods are used by an organization as the primary or only way of delivering such alerts and directives, care must be taken to ensure that this delivery system cannot be blocked, disrupted, or manipulated by an adversary in order to facilitate a cyberattack on the device's host.

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. Such controls are considered below.

A. Procedures for information retention

Individuals and organizations may be required to retain some information that is received, generated, stored, or transmitted by neuroprosthetic devices for legal, ethical, or practical reasons.[248] Note that some kinds of neuroprosthetic devices that mimic or interface with the natural biological memory systems of the human brain may store information in a way that is subject to significant compression, distortion, and degradation over time.[249] While storing information in our natural biological memory systems has, throughout human history, often been the best or only way of storing such information, the use of neuroprostheses that demonstrate such functional limitations may not be legally, ethically, or operationally advisable in cases when more effective and reliable storage mechanisms are available.

---

[247] Regarding security alerts, advisories, and directives, see *NIST SP 800-53* (2013), p. F–224.

[248] For a discussion of information retention policies and procedures, see *NIST SP 800-53* (2013), p. F–230.

[249] Regarding questions surrounding the nature and quality of long-term memory storage in the human brain, see Dudai (2004).

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

B. Sanitization of media prior to reuse or disposal

Neuroprosthetic devices or component storage units removed from a human host may contain confidential information about the host's biological processes and sensory experiences that must be cleared, purged, or destroyed before the device can be released for reuse or disposal.[250] Destruction of a storage medium may not be necessary if it can be guaranteed that the information cannot be retrieved from the medium or otherwise reconstructed. In the case of storage media contained within neuroprosthetic devices implanted within a human host, it may be impractical, illegal, and unethical to attempt to erase, purge, or destroy a storage medium without (or potentially even with) the host's permission.

Conclusion

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

[250] Regarding media sanitization, see *NIST SP 800-53* (2013), pp. F–122-23.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.

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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

Edlinger, Günter, Cristiano Rizzo, and Christoph Guger. "Brain Computer Interface." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, pp. 1003-17. Springer Berlin Heidelberg, 2011.

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

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

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

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

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

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

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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

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

Grottke, M., H. Sun, R.M. Fricks, and K.S. Trivedi. "Ten fallacies of availability and reliability analysis." In *Service Availability*, pp. 187-206. Lecture Notes in Computer Science 5017. Springer Berlin Heidelberg, 2008.

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

Considerations, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, pp. 113-34. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mitcheson, Paul D. "Energy harvesting for human wearable and implantable bio-sensors." In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE,* pp. 3432-36. IEEE, 2010.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).

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

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

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

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

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

Pribram, K.H., and S.D. Meade. "Conscious Awareness: Processing in the Synaptodendritic Web – The Correlation of Neuron Density with Brain Size." *New Ideas in Psychology* 17, no. 3 (1999): 205-14.

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

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

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

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

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

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

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

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

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

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

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

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

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.]

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
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.

"Preventive Security Controls for Neuroprosthetic Devices and Information Systems," Chapter Six in
Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics (Second Edition), pp. 178-247.
Indianapolis: Synthypnion Academic, 2017. ISBN 978-1-944373-09-2 (print edition) and 978-1-944373-10-8 (ebook).