"Managing security uncertainty with emerging technologies: the example of the governance of neuroprosthetic research"

Benjamin Farrand

Abstract

The governance of security in fields typified by emerging technologies is a complex and uncertain task. The very nature of an emerging technology means that its success as an innovation, as well as its implementation, dissemination and use, are highly speculative, as are the potential security threats or opportunities that it may present. Using the case study of the development of neuroprosthetics, a highly innovative yet experimental form of prosthetic limb that connects into nerve and muscle tissue, this chapter will explore how insights from science and technology studies concerned with managing risk and uncertainty can inform governance in areas of emerging technology. This chapter will demonstrate that existing legal frameworks are not well suited to providing governance solutions, and that instead a form of experimentalist governance based in principles of responsible research and innovation, allowing for organic and iterative forms of governance based on the interaction between knowledge and expertise provided by scientific researchers engaging with policy makers, agencies and civil society organisations are likely to be the norm until a technology is effectively realised and implemented – only then can more concrete governance structures be developed, as the lacunae of knowledge, certainty and appropriateness of response are bridged.

Introduction

This chapter seeks to analyse the challenges facing the management of security uncertainty in the European Union context, centring on the question *'how can policy-makers govern an emerging technology from a security-related perspective, when their successful implementation, dissemination and use are largely speculative?'* New and emerging technologies have the capacity to be highly disruptive. This is not intended in the sense of 'disruption' that is often used as a 'buzzword' in the context of Silicon Valley-based start-ups, grounded in an idea of Schumpeterian 'creative destruction' (Markides, 2006; Gobble, 2015) in which one business model is replaced by another. It is rather in the sense that these disruptive technologies can lead to unprecedented, unforeseen, and even transformative

changes to society and the economy. The McKinsey Global Institute (2013: 3) has identified four characteristics that disruptive technologies possess: 'a high rate of technology change, broad potential scope of impact, large economic value that could be affected, and substantial potential for disruptive economic impact' (see also the introduction to this book, Calcara, Csernatoni and Lavallée, 2019). However, when 'disruptive' technologies are discussed, it is often in terms of the potential benefits and opportunities they present (and predominantly economic at that), with comparably less consideration given to the possible detriments. When considered, the focus is predominantly upon their impact on current forms and levels of employment (for an excellent consideration of the role of disruptive technologies on workers, and the "gigification" of the economy, see Prassl, 2018). Even less discussed, when a technology is emergent, are the security risks (or opportunities) that they may present. This is not so surprising – an emerging technology is by its nature speculative, both in terms of its likelihood of success, as well as its conceivable social, economic and security impacts (Hoerr, 2011).

Examples of this include nanotechnology, which became the centre of significant debate and controversies as the technologies developed and could be realised (Macnaghten, 2010), or more recent discussions over blockchain technologies, the value of which is so far still unconfirmed, despite both media and academic speculation as to its future uses. In the early, formative stages of an emerging technology, research and discussion centre on its positive potential, rather than the negatives, as noted by Cordeiro et al. (2013). When a technology matures, and emphasis is placed on the innovation and dissemination of a technology, then there is an increased attention on possible security threats and opportunities, which may also feature in European Union (EU) funded research (Csernatoni, 2019). Until such a time, however, these technologies exist in a legal, policy and knowledge lacuna, making the management of any security risks they may potentially create difficult to conceptualise and therefore implement. Hence, it will be demonstrated in this chapter through the use of a case study of a highly speculative and newly emergent technology, neuroprosthetics, that the inherent uncertainties when dealing with an untested invention make their security governance particularly complicated. Neuroprosthetics are artificial limbs or organs connected into nerve or muscle tissue that allow for the regaining of use, and even sensation for individuals that have suffered limb damage as a result of injury or disease. However, they are at a very early stage of development, meaning that the focus of research is on the 'proof of concept' of the technology, and its application in impaired individuals, rather than a

detailed consideration of their broader social, economic and security risks. Neuroprosthetics, and in fact biotechnological inventions more generally, are not generally framed in explicit security terms, but as technologies with the potential to present security concerns.

The first section of this chapter will provide further exploration of the purpose, use and science behind neuroprosthetics, as well as the inherent unforeseeability of the security implications of these technologies. The second section of the chapter will analyse the existing legal framework that may serve to govern their use and implementation, indicating the lacuna in which these devices exist, and the difficulties in establishing a clear and effective legal regime for any security risks they may present. The third section of the chapter will then evaluate the dynamics of governance of emerging technologies more generally, and as applied to neuroprosthetics specifically, indicating how at these formative stages, knowledge gathering and reflective practice are key to understanding what potential risks and security threats may be posed by new disruptive technologies, and how the EU has attempted to provide for better understanding of the social, economic and security-related risks of new technologies through its Responsible Research and Innovation (RRI) approach. As the chaper will conclude, in areas of high uncertainty, low knowledge and in situations where a multitude of actors may be interested in the way in which a technology is governed, experimental governance is likely to emerge as a response to these uncertainties. Through networks of actors ranging from policy-makers and legislators to academic researchers, industry and civil society organisations, a more careful, nuanced and potentially future-proof approach to the governance of security risks posed by neuroprosthetics could be made more likely.

Background on neuroprosthetics

According to the World Health Organization, as of 2006, more than one billion people worldwide suffer from neurological conditions impacting upon limb usage, ranging from injury or trauma, Parkinson's disease, Alzheimer's and multiple sclerosis (2006: 178). Furthermore, the increase in the incidence of diabetes mellitus type II-related neuropathy and subsequent amputations is leading to a reversal in the decreases of lower-limb amputations being carried out. According to the most recent available statistics, in the US in 2008, it was determined that in 2005 there were 1.6 million individuals living with the loss of a limb, 38% of which were the result of diabetes-related vascular disease, figures estimated to increase to

3.1 million by 2050 (Ziegler-Graham et al., 2008: 427). While comparable figures are not available for the entire European Union, approximately 58 million people have diabetes in Europe, of which 90% are type II (European Commission, 2017a). According to Behrendt et al., diabetes is indicated in approximately half of amputations conducted in several countries in the EU, with incidence varying between 20% in Finland, to up to 75% in Slovakia (2018: 392). With these increases in diabetes and diseases such as Parkinson's and Alzheimer's, research in healthcare is becoming predominantly focused on the treatment of diabetes and these neurological conditions, along with the development of improved prosthetic devices for individuals rendered disabled by injury or disease. One promising avenue for this research and development is the creation of robotic limbs able to connect to nerve and muscle tissue, known as neuroprosthetics.

Neuroprosthetics have been defined as 'artificial devices designed to generate, restore or modulate a range of neutrally mediated diseases' (Glannon, 2016: 1–2). Neuroprosthetic limbs are the result of a distinct field of neuroprosthetic research, facilitated by separate and distinct developments in neuroscience and robotics, making it possible to develop brain-controlled artificial limbs capable of restoring fine motor skills and a sense of touch to individuals affected by disease or serious injury (Berger, 2019: 269). Operating through a brain-machine interface, signals coming from the brain's cortical neurons can be transformed into signals that can be interpreted by a computer system to move an external device. As the brain adapts to sending these signals, brain-machine interfacing improves, allowing for smoother, more nuanced manipulations of, for example, a robotic arm (Schweikard and Ernst, 2015; Eapen et al., 2017; Perlmutter, 2017). Recent innovations have allowed for the insertion of electrodes in the form of an intracortical brain-machine interface at the point of cervical spinal cord injury and a functional electrical stimulation device in a paralysed arm, allowing for a tetraplegic individual to successfully drink coffee from a self-controlled mug after 463 days, and to feed himself after 717 (Ajiboye et al., 2017). Neuroprosthetics have additional realised and emergent therapeutic benefits such as restoration of a sense of touch, as well as mitigating the effects of 'phantom limb syndrome', in which an individual experiences sensation of pain in a non-present limb (Blumberg and Dooley, 2017; Bartolozzi, 2018). While it may be assumed that the majority of this research is conducted in the US, there have been some significant breakthroughs in neuroprosthetic technology in the EU, with Horizon 2020 funded projects SensAgain, which has focused on restoring sensory-motor functionality and the ability to 'feel' the artificial limb as part of their body while striving to

eliminate phantom limb syndrome (SensAgain Project, 2016), and INPUT, specialising in upper-limb prostheses control systems intended to improve brain-machine interfaces allowing for increased dexterity and limb manipulation (INPUT, 2018).

As stated above, neuroprosthetics, and in fact biotechnological inventions more generally, are not generally framed in explicit security terms, but as technologies with the potential to present security concerns. This is a reflection of two interlinked factors; the first is that due to their nature as therapeutic interventions, the predominant focus of research and writing pertains to healthcare and disability, including the treatment of disability in law (see for example Bockman, 2009; Rosenfeld et al., 2008; Hanrahan, 2015; Wright and Fins, 2016). The second factor is the inherent uncertainty in determining the implications or consequences of many of these technologies, insofar as not only are the technologies themselves emergent, but so too are the social and economic impacts. Academic writers have focused on various different risks, social and ethical, that are potentiated by the use of advanced neuroprosthetics, should they reach that stage of development. In terms of security threats, there has been consideration of the potential dual use of neuroprosthetics for enhancement as well as therapy in the military, by creating an enhanced form of solider (Girling et al., 2017), the potential for 'brain-hacking' and a need for neurological security in the context of brain-machine interfaces (Denning et al., 2009), or even the blurring of the lines between cybercrime and physical assault through attacks against human-embedded systems such as neuroprosthetics (Gasson and Koops, 2013). Yet one commonality that this scholarship possesses is the frequent use of the words 'could' and 'potential'. Due to the inherently speculative and emergent nature of these technologies, the security risks they are likely to pose are equally speculative, making formalised governance difficult. How can policy makers therefore effectively govern the security risks of a speculative technology?

The security governance of neuroprosthetics: the limitations of legislation in combatting uncertainty

The management of these emerging and experimental technologies lies in an uneasy nexus between formal, legally binding rules, informal cooperation mechanisms and experimentalist governance (Sabel and Zeitlin, 2012). Experimentalist governance can serve as a template for the governance of new areas (Sabel and Zeitlin, 2012: 9), and the security dimension of emergent technologies is perfectly suited as a sector for this experimentation to arise (see for

example Kuhlmann et al., 2019), given its strategic uncertainty and the polyarchic power distributions, in which those with information and expertise (predominantly researchers) must engage with policy-makers, industry and other stakeholders, and with no one body having ultimate control or say (Sabel and Zeitlin, 2012). In order to demonstrate the requirement for experimentalist governance in this field, it is first necessary to detail the somewhat ill-fitting nature of existing and applicable EU legislation. In terms of legally binding rules, the nature of prosthetics means that they are classified as "medical devices" under the EU Medical Devices Regulation, which comes into effect in May 2020 (Regulation No 2017/754, 2017). According to Article 1, the European Regulation applies to the marketing, sale, distribution and putting into use of medical devices intended for human use, including clinical investigations concerning their use. For the purposes of neuroprosthetics, Article 2 defines a medical device as:

> 'any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings…[for the] diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability.'

Neuroprosthetics are categorised as a Class III device under Annex VIII Rule 6, as they are 'intended specifically for use in direct contact with the heart or central circulatory system or the central nervous system'. In terms of security, while there are five references to security mentioned in the Regulation, they refer to information security for any software built into the implantable device (Annex I, Chapter I, Section 17), and the security of clinical data from breach (Annex I, Chapter II, Section 4). Furthermore, and as shall be discussed further, rather than prescriptive legal requirements, the security obligations that *do* exist are framed in terms of best practices and setting of minimum requirements. Similarly, in terms of the security dimension of the proprietary information upon which the neuroprosthetic is based, the EU provides for comprehensive legal protection under its intellectual property laws, ranging from the Information Society Directive (Directive 2001/29/EC, 2001) for protection of any copyright in computer code serving to facilitate the brain-machine interface, the Trade Mark Regulation (Regulation No 2017/1001, 2017) for any trade marks registered in association with the neuroprosthetic for names, logos and etc., as well as patents registered in the Member States over the invention itself on the basis of national laws or the European Patent Convention. Similarly, and confidential information regarding the neuroprosthetic and

associated research may be protected by the Trade Secrets Directive (Directive 2016/943, 2016) as confidential business information prior to the registration of a patent. This provides for comprehensive protection of the intellectual property rights inherent in the design, which can be framed as ensuring a form of economic security for the company or undertaking involved in a neuroprosthetic's commercial development.

Yet such measures, under both the Medical Devices Regulation and the intellectual property framework, constitute a narrow perception of security based in the protection of information arising from neuroprosthetic research and development, as well as the ethics of the research involving human participants. The existing legal framework does not provide for a broader conceptualisation and understanding of security at a societal level arising from their use, indicative of the difficulties of formally regulating areas of emerging technological typified by uncertainty (see for example Weimer and Marin, 2016). In particular, emerging technologies often result in a period of 'regulatory disconnection' (Brownsword, 2012: 66), in which a technology may have outrun its regulatory framework. In such a scenario, the rules that may have ordinarily been applicable to such a technology (or type of technology) do not appear sufficient to regulate new uses of that technology or rapid advancements in its design or functionality. Indeed, new technologies suffer from what is referred to as the Collingridge dilemma (Collingridge, 1981), in which during the early stages of a new technology's development and application, regulation is difficult due to a lack of information regarding that technology's impact. However, once that technology becomes commonplace and entrenched in science, industry or business, any revision to that regulatory regime is both potentially expensive and resisted. For this reason, as Moses argues, those seeking to regulate an emerging technology need to act at an early stage, 'when the situation is more malleable' (Moses, 2015: 8). Though, providing a robust regulatory framework is difficult when the impact of a particular technology is uncertain. This results in an 'uncertainty paradox' (Asselt and Vos, 2006) in the regulatory sense, as it is deemed important to regulate before the technology becomes entrenched, yet determining the scope and function of that regulation is complicated by a lack of knowledge. For Easterbrook (1996), at this juncture, legislators must be careful to avoid a scenario in which they try to pull separate threads together in order to create a unified 'law of the horse'. A horse is a living thing, and so may be protected by laws concerned with animal welfare. Its sale, in turn, may be regulated by contract law, and its ownership by property law. Its use for sports such as horse-racing may in turn be regulated by specific legislation concerning competition and betting, and should the horse cause an

accident through negligently riding it at speed through a crowded street, this action may be governed by tort, or even criminal law. Yet these laws do not need to be brought together in a comprehensive law regulating horses. So too should it be ensured that legislation is not dependent on the technology in question, insofar as the utility of a 'law of the neuroprosthetic' is unlikely to be beneficial. Indeed, as discussed by Hildebrandt and Tielemans (2013), law should strive to be technology neutral, considering the social or economic problem that the technology raises, rather than the technology itself. This is the view that was taken by the European Commission in the late 1990s, when it concluded that its audiovisual policy reforms proposed in light of the development of Internet streaming should be technology neutral (1999: 10). However, as Hildebrandt and Tielemans (2013) continue, this technology neutrality may require additional legislative interventions in order to ensure that the technology is specifically regulated in a neutral way that nevertheless addresses a perceived risk (in their argument regarding data protection, to human rights), safeguards innovation, and achieves sustainability by 'future-proofing' law through the drafting of laws at appropriate levels of abstraction, guaranteeing that the law is not quickly rendered obsolete.

In the field of security, one such example is the implementation of the Network and Information Security Directive (2016), which requires Member States to provide for high levels of protection for critical information infrastructures from cyber-attacks, with the emphasis placed upon system resilience and the reporting of security breaches. The legislation does not specify the exact nature of cyber-attacks and provides for a deliberately broad definition of network and information systems. Nevertheless, in order to ensure that the parties with obligations under the Directive are identified, it was necessary to provide for a definition of 'providers of essential service and digital service providers' which is covered by Annex II, including entities such as energy providers, financial services providers and a specific list of digital infrastructure providers. Should these change, by means of new energy technologies beyond oil, electricity and gas, or new types of digital infrastructure, then arguably the legislation would not apply. Similarly, neuroprosthetics would not fall under the heading of providers of essential services and digital service providers, and arguably would only fall within the remit of the Directive should their use be targeted at initiating a cyber-attack against these critical infrastructures. Would this be possible, and are neuroprosthetics sufficiently regulated in terms of security in this field? It is very difficult at this time to say, but one would suggest not. Such endeavours still fall within the uncertainty paradox – when

the technology is only just emerging, and its potential unexplored, what are the risks, and what level of abstraction should be afforded in any legislative regime? Furthermore, when considering security, which is predominantly concerned with the protection from threats and prevention of incidents rather than seeking legal redress should a negative event occur, these uncertainties become harder to legislate for. In this lacuna, between knowing and unknowing, or rather, certainty and uncertainty, alternative and indeed, less formal modes of governance are instead pursued.

Emerging informal security cooperation in neuroprosthetic research: the beginning of experimentation?

One potential reason that law alone is perhaps ill-suited to resolve some of these tensions between innovation, security and uncertainty is that law often perceives science as an objective field of binary answers – something is scientifically proven or unproven, risky or safe. This is not the view shared by scholars in Science and Technology Studies, however, which presents a more critical reflection of the role of science in society. As Jasanoff (1990: 7) has stated, 'the questions regulators need to ask of science cannot in many instances be asked by science… in the absence of sufficient hard evidence, decisions have to be made on the basis of available facts supplemented by a large measure of judgment'. One such example is the use of assisted reproductive technologies, where in the absence of an absolute scientific certainty, a governable reality is constructed through the integration 'of the political, social, legal, ethical, bureaucratic, medical, technical and, quintessentially personal domains' (Sismondo, 2009: 67). After all, as Sismondo (2009: 68) states, before scientific knowledge stabilises, disagreement is the rule, not the exception. Conflict *between* scientific experts can be based not only on empirical observations, but the different cultural, historical, political and social backgrounds of the scientists that impact upon how they perceive a particular technology and its social implications (McCarthy, 2016; Rao et al., 2016). For this reason, faith in an objective and relatively incontestable 'science' is misplaced.

Furthermore, this perception of objective science complements a self-critique that appears to permeate legal understandings of science and emerging technologies. This critique is that while science moves incredibly quickly, law is slow and reactive, and therefore cannot keep up with developments (see Braverman, 2018). Instead, as Flear (2013) argues, the relationship is more nuanced – rather than playing catch-up with rapidly advancing

technologies, law can play a leading role by orienting, shaping and directing the conditions of possibility for the development and market availability of emergent technologies. These twin misperceptions however, namely the objectivity of science and law's inability to keep-up with emerging technologies, serve to frame the processes by which these new technologies are governed, and by which actors. One purpose behind the governance of risk is to mitigate uncertainty as far as possible (see for example Rosa et al., 2015; see also Renn and Klinke, 2019: 204). Evaluating an uncertain risk requires consideration of trade-offs, both in terms of risk versus benefit, but also risk versus risk, requiring mediation between different actors concerning acceptable, tolerable and intolerable risk; in the field of technology, this can include consideration of occupational safety, routine emissions of waste into air soil or water, or of accidents with sudden emission of energy and/or material (Renn and Klinke, 2019: 208–210). In the EU, this takes the form of reliance on expertise, and indeed networks of experts, in order to draw up guidelines for research, gather information, and assess risks through technology and impact assessments. The framework for this to be done is the non-legally binding mechanism of the Commission's 'Responsible Research and Innovation' (RRI) approach under the Horizon 2020 funding system, which focuses on multi-stakeholderism, the accumulation of knowledge regarding the outcomes of scientific research and actions, the ability to evaluate outcomes and opportunities in terms of societal needs and moral values, and to subsequently use these as functional requirements for the design and development of new research, products and services (European Commission, 2013: 5). These stakeholders range from policy makers, regulators and standardisation organisations to scientists, ethicists, civil society organisations and business/industry representatives (European Commission, 2013: 20).

Under RRI, the Commission works through informal modes of governance (on this, see generally Christiansen and Neuhold, 2013; see also Kleine, 2014) such as the coordination of Member State activities such as identifying objectives, roadmaps and benchmarks, along with encouraging the adoption of voluntary codes of conduct and standardisation, based on the information gathered by the networks of actors involved in identifying the social, ethical and economic impacts of emerging science and technologies (European Commission, 2013: 29–35). This, the Commission (2013: 49) reasons, would allow for the development of dynamic and flexible approaches to new technologies that a legislative initiative would lack. It must be stated however, that security is not a topic that tends to be the exclusive focus of these networks of stakeholders; instead, it is one of many topics that may be discussed within the

context of RRI, which also include issues such as justice, sustainability, democracy and efficiency (European Commission, 2013: 56).

Furthermore, as an interim report on Horizon 2020 found, within the context of the societal challenges identified as subjects for funding, security gained only 2.3% of the overall funding available, the smallest share recorded (European Commission, 2017b: 126). While by 2019 this has changed somewhat with an additional €2 billion in funding being made available for the purposes of security research, the deadline for which closed in August 2019, these projects tend to be divided into discreet packages such as cyber-security, the security of smart cities, or protection against natural disasters.

In the context of disruptive technologies more generally, neuroprosthetic technologies can be considered a form of 'pioneering' research, with low ecosystem embeddedness, with the emphasis being on achieving 'breakthroughs' rather than systematic diffusion or incremental innovation (European Commission, 2017b: 120). These are projects that have significant risks of failure, as well as uncertain futures. For this reason, less emphasis is placed upon considering their real-world application, including in the field of security. As the Interim Evaluation makes clear, many technology-related research projects are measured in terms of success based on traditional indicators, both by institutions and by researchers, such as prototypes, patents applied for, published outputs etc, rather than 'their impacts on e.g. decreasing CO2 emissions, improving health of citizen, or their security, often on the longer term' (European Commission, 2017b: 18). By way of example, the INPUT project mentioned earlier, does not mention security in any of its identified work packages. Similarly, SensAgain does not discuss security explicitly in its work, which is focused on getting an experimental and emerging technology to function. The Human Brain Project, a more advanced research project that is part-funded by the EU and began in 2013, has given some consideration to security in its discussion of brain-machine interfaces, but has made it clear that these security concerns are very much emergent and not particularly well understood at this stage; these emergent technologies are discussed in terms of their *potential* to reinvigorate debates over ethics, privacy and computer security, with 'perhaps the major ethical challenges [will] arise in human-machine integration' (Rose et al., 2016: 26). However, due to the emergent and speculative nature regarding their application, use and feasibility, there is currently a lacuna in which their conceptualisation as a security issue,

either in terms of presenting security threats, or indeed, security opportunities is not prevalent in EU discourse.

This does, however, present an opportunity. Given the flexibilities built into RRI as a concept and the absence of legally binding commitments, RRI can serve as a basis for policy experimentation. According to a meta-analysis conducted by Burget et al. (2017: 14), the definition and dimensions of RRI are still being formulated, but that common themes appear to be inclusion, anticipation, responsiveness and reflexivity. This allows for a wide range of stakeholders representing different interests and concerns to be part of the discussion regarding how 'research and innovation can or may benefit society as well as prevent any negative consequences from happening' (Burget et al., 2017:. 15). Florin (2019) argues that RRI can serve to complement risk governance, linking risk to responsibility, and providing a normative framework for the governance of specific risk issues. Through the necessity of experimentation and iterative governance design given the uncertainties of neuroprosthetic security risks, scientific research teams operating within the context of RRI can serve as informational nodes and helping to make the unknown less uncertain, as well as providing ideas as to how a technology may be appropriately implemented, disseminated and used. This allows for the emergence of a range of possible solutions, any of which may result in the formation of a crystallised governance structure, including the possibility of binding legislation. As one example of this experimentation, the previously mentioned Human Brain Project recently published some speculative considerations on the regulation of dual use technologies with security implications, concluding that the EU should consider extending its focus beyond the aims and objectives of the researchers involved in the project to the explicit consideration of the potential militarisation or securitisation of these technologies and the subsequent risks for peace and stability where they are exploited in those capacities (Aicardi et al., 2018: 18). How to achieve this? Hasselbalch (2018: 1870) suggests a more nuanced approach to assessing new technologies going beyond impact assessments and technology assessments to consider innovation assessments as iterative processes of understanding a technology and its social impacts, allowing for policy-makers to make 'effective and legitimate policy that manages to balance the viewpoints, interests and knowledge of attentive publics and experts'. This in turn would allow for the development of governance networks that could then determine how the security risks posed by these new technologies could be addressed – formalised cooperation through agencies such as the European Union Network and Information Security Agency (ENISA), Europol and the European Centre for

Disease Prevention and Control, for example, with their networks of sector experts and national regulators, through expert committees, through binding regulatory mechanisms such as Directives or Regulations, or a combination of all three, with feed-in from relevant public stakeholders such as disability activist groups, charitable commissions and national medical regulators.

Conclusions

As this chapter has sought to demonstrate, emerging technologies can be highly disruptive due to their uncertain application and the security risks they present. In such scenarios, the effectiveness of hard, legally-binding regimes is brought into question, and the best way to govern a new technology such as neuroprosthetics is ultimately unknown. In this context, experimentalist governance, drawing in a range of actors from science, research, policy and the public can help to better identify risks and uncertainties, and through policy experimentation, find effective ways of managing the security risks presented by these new technologies. In such a situation, the uncertainty can act as an opportunity, in which different models of governance can be applied to that technology, through reflexive use of innovation assessments as iterative processes, rather than 'end-stage' proposals for regulation, allowing for the governance of security threats to be more reflective, nuanced and carefully thought out. The EU's RRI approach to funding for Horizon 2020 projects, and the increased focus placed on the social implications of new technologies provides an opportunity for an approach to technology security governance that moves away from the binaries of 'objective' perceptions of science, incorporating the insights from Science and Technology Studies that allow for better understanding of the constructed nature of science, new technologies, and the risks they present.

References

Aicardi, C., Bitsch, L., Badum, N.B. and Datta, S. (2018), *Opinion on 'Responsible Dual Use': Political, Security, Intelligence and Military Research of Concern in Neuroscience and Neurotechnology*, The Human Brain Project, pp. 1–21.

Ajiboye, A.B., Willett, F.R., Young, D.R., Memberg, W.D., Murphy, B.A., Miller, J.P., Walter, B.L., et al. (2017), "Restoration of reaching and grasping movements through brain-

controlled muscle stimulation in a person with tetraplegia: a proof-of-concept demonstration", *The Lancet*, Vol. 389 No. 10081, pp. 1821–1830.

Asselt, M.B.A. van and Vos, E. (2006), "The Precautionary Principle and the Uncertainty Paradox", *Journal of Risk Research*, Vol. 9 No. 4, pp. 313–336.

Bartolozzi, C. (2018), "Neuromorphic circuits impart a sense of touch", *Science*, Vol. 360 No. 6392, pp. 966–967.

Behrendt, C.-A., Sigvant, B., Szeberin, Z., Beiles, B., Eldrup, N., Thomson, I.A., Venermo, M., et al. (2018), "International Variations in Amputation Practice: A VASCUNET Report", *European Journal of Vascular and Endovascular Surgery*, Vol. 56 No. 3, pp. 391–399.

Berger, K.M. (2019), "Emerging and Enabling Technologies in Biodefense", in Singh, S.K. and Kuhn, J.H. (Eds.), *Defense Against Biological Attacks: Volume I*, Springer International Publishing, Cham, pp. 253–281.

Blumberg, M.S. and Dooley, J.C. (2017), "Phantom Limbs, Neuroprosthetics, and the Developmental Origins of Embodiment", *Trends in Neurosciences*, Vol. 40 No. 10, pp. 603–612.

Bockman, C.R. (2009), "Cybernetic-Enhancement Technology and the Future of Disability Law Note", *Iowa Law Review*, No. 4, pp. 1315–1340.

Braverman, I. (2018), "Editing the Environment: Emerging Issues in Genetics and the Law", in Braverman, I. (Ed.), *Gene Editing, Law, and the Environment: Life Beyond the Human*, Routledge, Abingdon, pp. 1–27.

Brownsword, R. (2012), "The shaping of our on-line worlds: getting the regulatory environment right", *International Journal of Law and Information Technology*, Vol. 20 No. 4, pp. 249–272.

Burget, M., Bardone, E. and Pedaste, M. (2017), "Definitions and Conceptual Dimensions of Responsible Research and Innovation: A Literature Review", *Science and Engineering Ethics*, Vol. 23 No. 1, pp. 1–19.

Christiansen, T. and Neuhold, C. (Eds.). (2013), *International Handbook on Informal Governance*, Edward Elgar, Cheltenham, U.K.

Collingridge, D. (1981), *Social Control of Technology*, Open University Press, Milton Keynes.

Cordeiro, J.L., Hauptman, A. and Sharan, Y. (2013), "Foresight of evolving security threats posed by emerging technologies", *Foresight*, available at:https://doi.org/10.1108/FS-05-2012-0036.

Csernatoni, R. (2019), "The EU's Technological Power: Harnessing Future and Emerging Technologies for European Security", in Baciu, C.-A. and Doyle, J. (Eds.), *Peace, Security and Defence Cooperation in Post-Brexit Europe: Risks and Opportunities*, Springer International Publishing, Cham, pp. 119–140.

Denning, T., Matsuoka, Y. and Kohno, T. (2009), "Neurosecurity: security and privacy for neural devices", *Neurosurgical Focus*, Vol. 27 No. 1, p. E7.

Directive 2001/29/EC. (2001), *Of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*.

Directive 2016/943. (2016), *Of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against Their Unlawful Acquisition, Use and Disclosure*.

Directive 2016/1148. (2016), *Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*.

Eapen, B.C., Murphy, D.P. and Cifu, D.X. (2017), "Neuroprosthetics in amputee and brain injury rehabilitation", *Experimental Neurology*, Vol. 287, pp. 479–485.

Easterbrook, F.H. (1996), "Cyberspace and the Law of the Horse The Law of Cyberspace", *University of Chicago Legal Forum*, pp. 207–216.

European Commission. (1999), *Communication: Principles and Guidelines for the Community's Audiovisual Policy in the Digital Age*, No. COM(1999) 657, Brussels, pp. 1–23.

European Commission. (2013), *Options for Strengthening Responsible Research and Innovation*, Brussels, pp. 1–78.

European Commission. (2017a), "Chronic diabetes affects millions of people in the EU",

Eurostat, 13 November, available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20171113-1 (accessed 25 September 2019).

European Commission. (2017b), *Commission Staff Working Document: In-Depth Interim Evaluation of Horizon 2020*, No. SWD(2017) 222 final, pp. 1–146.

Flear, M.L. (2013), "Regulating New Technologies: EU Internal Market Law, Risk, and Socio-Technical Order", in Flear, M.L., Farrell, A.-M., Hervey, T.K. and Murphy, T. (Eds.), *European Law and New Health Technologies*, OUP Oxford, Oxford, United Kingdom, pp. 74–120.

Florin, M.-V. (2019), "Risk governance and 'responsible research and innovation' can be mutually supportive", *Journal of Risk Research*, pp. 1–15.

Gasson, M.N. and Koops, B.-J. (2013), "Attacking Human Implants: A New Generation of Cybercrime", *Law, Innovation and Technology*, Vol. 5 No. 2, pp. 248–277.

Girling, K., Thorpe, J. and Auger, A. (2017), *A Framework to Assess the Military Ethics of Human Enhancement Technologies*, No. DRDC-RDDC-2017-L167, Defence Research and Development Canada, pp. 1–18.

Glannon, W. (2016), "Ethical issues in neuroprosthetics", *Journal of Neural Engineering*, Vol. 13 No. 2, pp. 1–22.

Gobble, M.M. (2015), "The Case against Disruptive Innovation", *Research Technology Management*, Vol. 58 No. 1, pp. 59-63

Hanrahan, D. (2015), "Neuroenhancement, Ethics & the Future of Disability Law", *Health Law Outlook*, Vol. 8 No. 1, pp. 1–17.

Hasselbalch, J.A. (2018), "Innovation assessment: governing through periods of disruptive technological change", *Journal of European Public Policy*, Vol. 25 No. 12, pp. 1855–1873.

Hildebrandt, M. and Tielemans, L. (2013), "Data protection by design and technology neutral law", *Computer Law & Security Review*, Vol. 29 No. 5, pp. 509–521.

Hoerr, R.A. (2011), "Regulatory uncertainty and the associated business risk for emerging technologies", *Journal of Nanoparticle Research*, Vol. 13 No. 4, pp. 1513–1520.

INPUT. (2018), "Mission Statement", *INPUT Horizon 2020*, available at: http://www.input-h2020.eu/the-mission/ (accessed 25 September 2019).

Jasanoff, S. (1990), *The Fifth Branch: Science Advisers as Policymakers*, Harvard University Press, Cambridge, Mass.

Kleine, M. (2014), "Informal Governance in the European Union", *Journal of European Public Policy*, Vol. 21 No. 2, pp. 303–314.

Kuhlmann, S., Stegmaier, P. and Konrad, K. (2019), "The tentative governance of emerging science and technology—A conceptual introduction", *Research Policy*, Vol. 48 No. 5, pp. 1091–1097.

Macnaghten, P. (2010), "Researching Technoscientific Concerns in the Making: Narrative Structures, Public Responses, and Emerging Nanotechnologies", *Environment and Planning A: Economy and Space*, Vol. 42 No. 1, pp. 23–37.

Markides, C. (2006), "Disruptive Innovation: In Need of Better Theory", *The Journal of Product Innovation Management,* Vol. 23 No. 1, pp. 19-26

McCarthy, D.R. (Ed.). (2016), *Technology and World Politics: An Introduction*, Routledge, Abingdon, Oxon.

McKinsey Global Institute. (2013), *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy*, pp. 1–176.

Moses, L.B. (2015), "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target", *Law, Innovation and Technology*, Vol. 5 No. 1, pp. 1–20.

Perlmutter, S.I. (2017), "Reaching again: a glimpse of the future with neuroprosthetics", *The Lancet,* Vol. 389 No. 10081, pp. 1777–1778.

Prassl, J. (2018), *Humans as a Service: The Promise and Perils of Work in the Gig Economy*, OUP, Oxford.

Rao, B., Gopi, A.G. and Maione, R. (2016), "The societal impact of commercial drones", *Technology in Society*, Vol. 45, pp. 83–90.

Regulation No 2017/754. (2017), *Of the European Parliament and of the Council of 5 April 2017 on Medical Devices*.

Regulation No 2017/1001. (2017), *Of the European Parliament and of the Council of 14 June 2017 on the European Union Trade Mark*.

Renn, O. and Klinke, A. (2019), "Risk governance: Concept and application to technological risk", in Burgess, A., Alemanno, A. and Zinn, J. (Eds.), *Routledge Handbook of Risk Studies*, Routledge, Abingdon, Oxon, pp. 204–215.

Rosa, E., McCright, A. and Renn, O. (2015), *The Risk Society Revisited: Social Theory and Risk Governance*, Temple University Press, Philadelphia, Pa.

Rose, N., Aicardi, C. and Reinsborough, M. (2016), *Future Computing and Robotics: A Report from the HBP Foresight Lab*, The Human Brain Project, pp. 1–46.

Rosenfeld, J., Bandopadhayay, P., Goldschlager, T. and Brown, D. (2008), "The Ethics of the Treatment of Spinal Cord Injury: Stem Cell Transplants, Motor Neuroprosthetics, and Social Equity", *Topics in Spinal Cord Injury Rehabilitation*, Vol. 14 No. 1, pp. 76–88.

Sabel, C.F. and Zeitlin, J. (2012), "Learning from Difference: The new architecture of experimentalist governance in the EU", in Sabel, C.F. and Zeitlin, J. (Eds.), *Experimentalist Governance in the European Union: Towards a New Architecture*, OUP, Oxford, pp. 1–28.

Schweikard, A. and Ernst, F. (2015), "Rehabilitation, Neuroprosthetics and Brain-Machine Interfaces", in Schweikard, A. and Ernst, F. (Eds.), *Medical Robotics*, Springer International Publishing, Cham, pp. 349–361.

SensAgain Project. (2016), "About SensArs Neuroprosthetics", *SensArs*, available at: http://www.sensars.com/about/ (accessed 25 September 2019).

Sismondo, S. (2009), *An Introduction to Science and Technology Studies*, 2nd edition., Wiley-Blackwell, Chichester, U.K.

Weimer, M. and Marin, L. (2016), "The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies", *European Journal of Risk Regulation*, Vol. 7 No. 3, pp. 469–474.

World Health Organization. (2006), *Neurological Disorders: Public Health Challenges*, WHO, Geneva, pp. 1–232.

Wright, M.S. and Fins, J.J. (2016), "Rehabilitation, Education, and the Integration of Individuals with Severe Brain Injury into Civil Society: Towards an Expanded Rights Agenda in Response to New Insights from Translational Neuroethics and Neuroscience", *Yale Journal of Health Policy, Law and Ethics*, No. 2, pp. 233–288.

Ziegler-Graham, K., MacKenzie, E.J., Ephraim, P.L., Travison, T.G. and Brookmeyer, R. (2008), "Estimating the Prevalence of Limb Loss in the United States: 2005 to 2050", *Archives of Physical Medicine and Rehabilitation*, Vol. 89 No. 3, pp. 422–429.