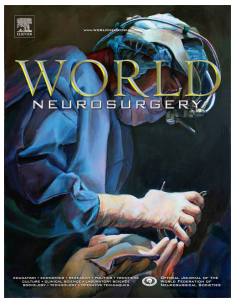
Accepted Manuscript



Brainjacking: implant security issues in invasive neuromodulation

Laurie Pycroft, MSc., Sandra G. Boccard, PhD., Sarah L.F. Owen, DPhil., John F. Stein, FRCP, James J. Fitzgerald, FRCS(SN), Alexander L. Green, FRCS(SN), Tipu Z. Aziz, FMedSci

PII: S1878-8750(16)30272-8

DOI: 10.1016/j.wneu.2016.05.010

Reference: WNEU 4071

To appear in: *World Neurosurgery*

Received Date: 8 January 2016

Revised Date: 4 May 2016

Accepted Date: 5 May 2016

Please cite this article as: Pycroft L, Boccard SG, Owen SLF, Stein JF, Fitzgerald JJ, Green AL, Aziz TZ, Brainjacking: implant security issues in invasive neuromodulation, *World Neurosurgery* (2016), doi: 10.1016/j.wneu.2016.05.010.

Brainjacking: implant security issues in invasive neuromodulation

Author names and affiliations

Laurie Pycroft, MSc.[1]; Sandra G. Boccard, PhD.[1]; Sarah L.F. Owen, DPhil.[3]; John F. Stein, FRCP; James J. Fitzgerald, FRCS(SN)[1]; Alexander L. Green, FRCS(SN)[1]; Tipu Z. Aziz, FMedSci[1]

1: Oxford Functional Neurosurgery, University of Oxford, Level 6, West Wing, John Radcliffe Hospital, Headington, Oxford, UK, OX3 9DU

2: Department of Physiology, Anatomy, and Genetics, Sherrington Road, Oxford, UK, OX1 3PT

3: Department of Applied Health and Professional Development, Oxford Brookes University, Headington Campus, Oxford, UK, OX3 0BP

Correspondence should be addressed to Laurie Pycroft

Email: laurie.pycroft@nds.ox.ac.uk Tel: +44 (0) 7788804011

Author contributions statement

LP, JJF and TZA developed the core concept of the review.

LP wrote the manuscript and identified the security risks specific to DBS.

SGB, SLFO, JFS, JJF, ALG, and TZA all reviewed the manuscript several times and provided extensive feedback and suggestions for rewrites based on their areas of expertise.

Keywords

Deep Brain Stimulation; Hacking; Implantable Pulse Generator; Implantable medical device; Cybersecurity; Medical device security; Neurosecurity; Brainjacking; Neurosurgery

Highlights

- Current state of information security of neurological implants is reviewed
- Specific risks associated with brain implant hacking (“brainjacking”) are identified
- Trade-offs between security and function of brain implants is discussed
- Recommendations are made for improving future security of neurological implants

Introduction

The concept of altering human conscious experience and behaviour *via* unauthorised manipulation of implanted electronic devices dates back to science fiction literature of the 1980s, when authors began to speculate about the advantages and pitfalls offered by hypothetical electronic neural implants[1,2]. Until recently the risk of neurological implants being used against their users was firmly in the realm of fantasy. However, the increasing sophistication of invasive neuromodulation, coupled with developments in information security research and consumer electronics, has resulted in a small but real risk of malicious individuals accessing implantable pulse generators (IPGs). Unauthorised access to IPGs could cause serious harm to the patients in whom the devices are implanted.

This review summarizes the current literature on the plausibility and potential impact of this risk, identifies possible physiological mechanisms of attack, and highlights trade-offs inherent in IPG design that provide exploitable vulnerabilities. In doing so we aim to raise awareness of neurological implant security and thereby stimulate discussion of defensive measures. Other than a very brief review from 2009[3], this article is the first to address medical implant information security threats in detail from a neurological/neurosurgical perspective.

For the purposes of this review, unauthorised control of an electronic brain implant will be referred to as “brainjacking”, analogous to the hijacking of a vehicle. The term “neurosecurity” is used to refer to defence mechanisms protecting neurological implants from subversion[3].

Plausibility and risk of brainjacking

Over 100,000 patients worldwide have received deep brain stimulation (DBS), predominantly for movement disorders[4]. This number is only likely to increase in the future as DBS shows promise for treating a wide range of neurological and psychiatric conditions[5,6]. More speculatively, DBS and

similar implants have been proposed as a potential tool for enhancing cognition in healthy individuals[7–9] and as a method of correcting "abnormal moral behaviour"[10]. Factors contributing to the increasing prevalence of DBS include reductions in treatment cost, increasing demand in newly industrialised countries, ageing populations in more economically developed countries, and ongoing improvements in IPG design[11].

With increasingly widespread adoption of these intracranial neuromodulation techniques comes greater opportunity for individuals with a high degree of technical competence to use the technology for malicious purposes. Information technology security researchers have demonstrated the potential for exploitation of the security limitations of implantable medical devices, with potentially severe consequences.

To date, two implantable medical devices have been exploited publicly – insulin pumps and implantable cardiac defibrillators. In 2011, Jay Radcliffe, a security researcher and diabetic, utilised publicly available device information and an inexpensive consumer-grade microprocessor with radiofrequency transmitter to bypass the security of an insulin pump, and outlined a potentially lethal method of attack[12]. This work was extended by Barnaby Jack, who demonstrated unauthorised control over an insulin pump at a distance of 90 metres without prior knowledge of the device serial number, a limitation of Radcliffe's earlier attack[13]. Jack further demonstrated unauthorised and potentially lethal control over an implantable defibrillator [14], a risk first outlined in 2008 by academic research[15]. As a result of this work, the FDA has issued a safety warning over the risks of inadequate medical device security[16] and public workshops have been undertaken in collaboration with industry to address the issue[17,18]. Most recently, the FDA has warned about intrusion vulnerabilities in a continuous external drug pump[19]. Furthermore, the United States Department of Homeland Security has issued an alert regarding the unacceptable risks associated with using hard-coded (unchangeable) passwords in medical devices[20].

Unauthorised access to implants can be lethal – deliberate misuse of an insulin pump (albeit not *via* electronic exploitation) has been reported in at least one murder[21] and US Vice President Dick Cheney reportedly had the wireless telemetry on his ICD disabled during his time in office for fear of political assassination[22]. Wireless exploitation of implants is also likely to be subtle – device failures are a somewhat common eventuality [23] and post-failure device diagnostics are rarely performed. Even if an attack were detected, tracking down the attacker would be a highly challenging task.

Attacks could be made for a variety of reasons including blackmail, malice against an individual, or manipulation of a politically notable individual. The motive need not even be rational; in 2008 a website for epilepsy sufferers was attacked using flashing images designed to trigger seizures[24], with the attackers' apparent motivation being amusement.

Similar security issues have been raised in the automobile industry, particularly in the wake of high-profile proof-of-concept hacks of several major vehicle brands[25]. The security research community has released a set of guidelines, the "Five Star Automotive Cyber Safety Program"[26], the principles of which may be translatable to neurosecurity design.

The information technology community has given some degree of recognition to medical implant information security vulnerabilities, as detailed in *Secure implant design*, but the topic has only been discussed seriously in the biomedical literature recently[27–29] and there are no detailed discussions of the risks specific to neurological implants beyond a single forward-thinking but brief review published several years ago[3].

Methods of attack

Once an attacker has successfully breached security on a device, they have several options for brain-jacking their victim. Stimulation parameters including voltage/current, frequency, pulse width, and electrode contact can be altered in order to change the effect of stimulation[30]. These potential

attacks are unlikely to be directly lethal, but may cause serious harm and distress. The list below is not exhaustive and, as the variety and complexity of invasive neuromodulation therapies increases, the potential methods of attack grow in number. Several of these attack strategies are highly speculative and could require a degree of physical or informational access that is unrealistic for most attackers. Clinicians should nevertheless be aware of these possibilities, especially as the complexity of neural implants increases, with a concomitant increase in the complexity and variety of available attack vectors. See Table 1 for an overview of potential attacks.

Blind attacks

The most straightforward attacks rely on no patient-specific knowledge on the part of the attacker, i.e. the attacker is "blind". Simply turning off the stimulation would result in a loss of therapeutic effect. If temporary, this would typically be no more than an annoyance as the patient would be able to re-initiate stimulation, although sudden cessation of stimulation can cause serious "rebound" symptoms in a variety of disorders including Parkinson's disease (PD), essential tremor (ET), and obsessive-compulsive disorder (OCD)[31–34]. More invasive attacks would allow permanent disabling of an IPG, necessitating surgical replacement of the device, with concomitant surgical risks and expenses.

Repeated interrogation of an implanted device can deplete the battery prematurely[35]. In the case of traditional non-rechargeable IPGs, this will result in reduced device lifespan; in the case of rechargeable models, repeated over-draining of the battery can result in the device disabling itself in order to avoid potential catastrophic failure (depending on IPG model). Battery damage would also necessitate IPG replacement.

Although the above forms of brainjacking would be unpleasant, their lasting effects would likely be minor. It would, however, be possible to induce tissue damage as a result of increasing pulse width and voltage. The firmware of most IPGs is designed to lock out dangerous stimulation parameters

under normal usage, but an attacker may be able to subvert these limits. Typical parameters for DBS induce minimal tissue damage[36–38] but feline *in vivo* data indicate that tissue damage can occur at high charge densities[39,40], with extrapolation from these data providing an estimate of safe stimulation parameters[41]. The effects of such electrically induced lesions would vary depending on location and extent of damage, but could result in serious disability.

Finally, an attacker could seek to gain information from the target's implant in a passive or active manner[27], i.e. by passively "listening" for information transmitted during normal operation or actively accessing the device to receive information. Most IPGs store some identifiable information including patient name, diagnosis, and physician details; all IPGs, by necessity, store information regarding stimulation parameters. Acquiring this information may be an ends in itself or may form the first stage of one of the targeted attack strategies detailed below.

Targeted attacks

More elaborate attacks could make use of implanted electrodes to alter behaviour and cognition by modifying stimulation parameters based on some degree of pathophysiological knowledge of the patient. Increasing or decreasing stimulation frequency has a substantial impact on the efficacy of DBS for several indications, in some cases reversing the positive effects of stimulation. Alteration of voltage or pulse width changes the volume of tissue activated (VTA)[30,42], which may diminish the treatment effect or induce unpleasant off-target effects by stimulating surrounding structures. Changing the electrode contact(s) used for stimulation would enable off-target structures to be stimulated directly, resulting in variable effects depending on electrode location and surgical approach used[43]. With the development of directionally selective electrodes, currently being introduced into clinical use[44], the intended increase in precision of on-target stimulation could also afford attackers more sophisticated control over malicious off-target stimulation.

These attacks may require sophisticated knowledge of the patient's clinical condition, making them more challenging to perform, although the effects are potentially more desirable from some attackers' perspective. A dedicated attacker may be able to acquire medical records *via* breaching medical databases, social engineering, or simple attacks as discussed above. Even without medical knowledge of the patient, scanning up and down stimulation parameters could enable an attacker to empirically determine settings that cause distress.

Impairing motor function

Movement disorders are the most common indications for DBS, with over 100,000 patients estimated to have undergone DBS for PD alone[4]. In both PD and ET there is potential for an attacker to subvert IPG function to impair motor control. In patients receiving DBS of the subthalamic nucleus (STN) for PD, stimulation at a frequency of ≥130 Hz typically results in desired clinical outcomes[45], whereas 5-10 Hz or ~20 Hz stimulation can significantly exacerbate bradykinetic/akinetic symptoms[46–49]. Similar effects have been reported in DBS of the internal globus pallidus for PD, wherein switching to more dorsal electrode contacts resulted in pronounced akinesia[50]. Given these data, an attacker may substantially impair motor function by altering basic stimulation parameters, thereby increasing the patient's parkinsonian symptoms beyond baseline levels. A similar potential attack exists for ET patients with DBS of the ventral intermediate nucleus, wherein low frequency, high voltage stimulation can significantly exacerbate tremor symptoms[51].

Inducing pain

DBS is an effective treatment for a wide range of chronic pain disorders, with most established techniques showing efficacy for focal pain[52], and emerging targets showing promise in the treatment of whole-body pain syndromes[53,54]. The periventricular/periaqueductal grey matter (PVG/PAG) and the ventral-posterolateral/ventral-posteromedial nuclei of the sensory thalamus (VPL/VPM) are the

most frequently targeted regions. In clinical practice, these nuclei are stimulated at low frequency to alleviate pain, but higher frequency stimulation, above ~70 Hz, is reported to increase painful sensations[54,55]. Alteration of stimulation frequency in this manner by an attacker could induce severe pain in these patients.

Altering impulse control

Impulse control disorders (ICDs), involving behavioural problems such as hypersexuality and pathological gambling, are a relatively common problem in patients with PD and are particularly strongly associated with the use of dopaminergic agonists[56,57]. In normal clinical practice, STN-DBS offers a mechanism for reduction of dopaminergic medication, thereby assisting in the management of ICDs[58,59].

Several case reports indicate that inappropriate electrode contact selection can induce a range of disturbances in impulse control. Mania, hypersexuality, and pathological gambling have been linked with specific electrode contacts[60–63]. The precise effects of a given contact will depend on a variety of factors – individual anatomical variation, surgical approach taken, other stimulation parameters, etc. – but it appears plausible that disruption of impulse control could be achieved in at least a subset of patients *via* switching of electrode contact. An attacker may be able to disrupt the clinician-set stimulation parameters and thereby remove protection from, or even induce, ICDs.

Modifying emotion and affect

Alteration of emotional processing and affect can occur during DBS, either as a side-effect or as part of the intended stimulation effects. Dysfunction of emotional behaviour has been noted in several case reports of patients receiving STN-DBS for PD, including pathological crying[64–66], inappropriate laughter[67], and affective lability[68]; likely due to off-target stimulation. Undesirable off-target

emotional effects have also been observed in patients receiving DBS of the nucleus accumbens (NAcc) for OCD, notably strong sensations of fear and panic with concomitant autonomic arousal[69–71]. Deliberate stimulation of inappropriate electrode contacts by an attacker may, therefore, induce personally and socially undesirable emotional changes, which would likely be highly distressing for a patient and their loved ones.

Modulating reward processing

Perhaps the most concerning attack strategy feasible using currently implanted neural devices involves the use of operant conditioning to exert substantial control over a patient's behaviour. As noted above, the NAcc is the target of stimulation in several emerging DBS indications, including depression, OCD, and anorexia. Currently the number of patients undergoing NAcc-DBS is small although this number may rise if one or more indications proves to be clinically viable.

The enhancement/attenuation of positive reinforcement effected by NAcc stimulation has been well demonstrated in humans and other animals[72,73] and, indeed, is a core component of the rationale for its value as a target in such a broad range of conditions[74–76]. Sufficient control over the IPG could enable use of operant conditioning to modify the behaviour of the victim, potentially reinforcing harmful behaviours. This strategy would require an even greater level of sophistication on the part of the attacker than required by most of the attacks discussed above. One would need continuous control over the IPG for an extended period of time, along with a means of surveillance over the victim. It would be feasible for the attacker to use a wireless relay device placed near the victim to remove the need to be in close physical proximity, but placing this device without detection would bring its own challenges.

Secure implant design

Several design constraints exist that necessitate trade-offs between neurosecurity and other desirable features of IPGs. These trade-offs and challenges, along with specific methods of attack and desirable security features for future devices, have been discussed in greater detail elsewhere[27–29,77–79], therefore this section will consider the factors most relevant to clinical practice – battery life and practicality.

Telemetric adjustment of IPG settings provides substantial benefits in terms of the flexibility and usability of the device[27], but also provides mechanisms by which the device may be subverted. To date, IPG telemetry has relied on near-field transcutaneous wireless communication between the implanted device and proprietary IPG-specific external telemetry devices, using several dedicated frequency bands, under the control of either clinician or patient. The newest IPGs utilise consumer-grade wireless communication protocols such as Bluetooth, and in the longer-term, device manufacturers are considering utilising communication over TCP/IP, enabling remote telemetric control and/or software updates of IPGs over the internet. Additionally, manufacturers are shifting from proprietary external hardware programmers (which are expensive to design, manufacture, and update) to proprietary software running on consumer devices such as tablets and smartphones.

Unfortunately, both proprietary and consumer protocols have drawbacks; proprietary systems typically attempt to make use of “security through obscurity”, i.e. maintaining secrecy about software/hardware design in order to thwart potential attackers, which is unreliable[79]. Proprietary designs are also typically less open to security researchers due to manufacturers’ reluctance to disclose trade secrets to third parties, which increases the challenge of uncovering security flaws. This challenge is exacerbated by the risk of lawsuits brought against legitimate security researchers for disclosing design flaws under legislation such as the Digital Millennium Copyright Act, as discussed in a recent guidance statement made by the Electronic Frontier Foundation to the FDA[80].

Conversely, popular consumer protocols are widely adopted and understood, potentially lowering the barrier of entry to attackers.

Emerging IPG technology will provide opportunities and pitfalls in terms of neurosecurity. One potential example is “closed-loop” or “adaptive” DBS, wherein physiological signals are used to alter stimulation profiles on the fly, without any intervention from patients or clinicians. These systems may plausibly be more resilient to brainjacking attempts, as the decreased requirements for human intervention would facilitate the use of less easily accessible programming methods than current IPG user interfaces, thereby increasing security without a concomitant decrease in system utility. Conversely, however, the increased complexity of closed-loop systems may provide additional surfaces for attackers to exploit. Certain experimental closed-loop systems utilise wireless interfaces between sensor, controller, and stimulation components[81,82]; use of such a design would effectively turn neuromodulation into a Supervisory Control and Data Acquisition (SCADA) system. By maliciously influencing the such a system’s input, it is possible to influence output parameters and thereby alter stimulation – a process that has been demonstrated to devastating effect in several real-world SCADA systems, most famously the Iranian nuclear fuel centrifuges that were damaged by malware called Stuxnet[83].

Several potential security solutions exist although, as detailed below, many are subject to limitations. Specific solutions include improved auditing[84], rolling code cryptography[77], server-based cryptographic key management[28], formal verification of device software[85], proximity-based authentication[86,87], and “communication cloaker” or “shield” wearable devices that mediate secure communication between programmer and implant[88,89]. For more detail, see Camara et al. (2015)[27].

It is the responsibility of IPG manufacturers to carefully trade-off between clinical demands, ergonomics, and neurosecurity. Designing any secure digital system is difficult and, as discussed below, IPG design presents several unusual challenges that are not easily solved without causing problems elsewhere in the system. Neuromodulation is a rapidly evolving field and it is difficult to

predict future innovations, so any regulatory approach to solving problems of neurosecurity must carefully balance information security risks with the risk of impeding technological development through application of inflexible rules. Manufacturers and regulators should endeavour to ensure that, when security flaws are found, researchers are able to disclose these flaws in a safe and timely manner without undue legal impediments[80].

Battery life

Most IPGs currently in use rely on a non-rechargeable battery, which can last anywhere from <1 year to a decade, depending on IPG model and stimulation parameters[90], necessitating surgery to explant and replace the depleted device. Given the risks and distress associated with surgery, manufacturers attempt to maximise the life of the battery by using the highest-capacity cells that are feasible and by minimising power drain resulting from the electronic systems.

A substantial portion of energy usage is taken up by the stimulation itself and is therefore unavoidable, but the rest is devoted to maintaining the function of the internal electronics of the device – microprocessor(s), memory, and wireless communication system. Most potential security improvements involve increased power drain from one or more of these components, or the inclusion of additional components that would contribute to energy usage. Cryptographic systems require extra processing power to encrypt/decrypt data[79], improved auditing requires more memory to be of value, and frequent software verification would result in increased wireless communications. Rechargeable IPGs are becoming increasingly popular and reduce the importance of battery life somewhat, but the limited charge/discharge cycles available to each battery and the desire to maximise time between charging still necessitate a careful approach to power management. Future closed-loop DBS systems may reduce power consumption in comparison to traditional IPGs[91], thereby freeing up more energy to be used for security systems.

Practicality

A crucial design consideration for any security system is the human factor. Human error is a major cause of security failures across many domains of information technology[92] and ergonomics is an important secondary concern in the development of medical devices[93]. If a security system requires too much time and effort on the part of patients and clinicians, there is risk that it will remain unused or, potentially worse, that it will be improperly used and thereby provide a false sense of security. Furthermore, in a medical context, ease-of-use and open access can be critical for proper treatment.

Most of the security solutions that would be implemented on the implantable device would not impact considerably upon the practicality of the system; a little extra time setting up proper security protocols during the initial programming stage is acceptable and, with adequate training, may be implemented reliably. Problems are more likely to arise with additional devices being added to the system, especially if patients are expected to use these devices constantly. Cloaker and shield devices have been proposed[88,89] – external electronic devices that provide an additional layer of security between the implant and other devices that are trying to communicate with it. These would likely provide a substantial improvement to system security, but would risk being under-utilised due to the inconvenience of carrying around additional devices. Excessively burdensome security systems may even incentivise non-adherence to treatment, resulting in re-emergence of a patient's symptoms. This inconvenience may be attenuated by integration of the security systems into consumer-grade electronic devices, e.g. by enabling a patient's smartphone to act as a communications hub[78], but using consumer devices in this manner raises yet more security concerns.

Device manufacturers are beginning to offer telemetric control of neural implants using consumer devices; several IPGs currently on the market offer integration with smartphone or tablet type

devices. This development may provide substantial benefits in terms of user friendliness and reduced clinical visits. However, enabling access to implants *via* internet-enabled consumer electronics risks attackers exploiting security flaws in these devices and thereby indirectly accessing and subverting implants. Remote network access vastly increases the availability of devices to attackers, making attacks easier and therefore more attractive. A 2015 FDA warning addressed security vulnerabilities in a network-accessible drug pump[19], demonstrating the risks associated with internet-enabled medical devices. This issue of network security in healthcare is discussed in detail in a recent paper by Independent Security Evaluators [94]

Notably, allowing wireless access to implants in this manner would enable over-the-air firmware updates, which are not currently implemented in any model of IPG. This would facilitate the patching of security holes (increasingly important for the longer-lasting rechargeable IPGs), but would also leave devices open to injection of counterfeit firmware updates[95]. Firmware serves to control the hardware of embedded medical devices such as IPGs, so any alteration to it would enable substantial changes to the function of the device, beyond the changes that are possible through the user interface. For example, while the user interface on most IPGs will prevent the setting of stimulation parameters capable of causing tissue damage (as discussed in “Blind attacks”, above), alteration of firmware may be able to bypass these restrictions, enabling attackers to cause lesions. Allowing IPGs to connect to the internet routinely would increase the probability of such illegitimate firmware modification by allowing attackers to access the devices remotely instead of requiring them to be in close proximity.

Manufacturers must carefully weigh these factors when deciding whether wireless interfacing is suitable for a given implantable device. An important consideration here is the context under which updates can take place and the authorisations necessary; it may be preferable to prevent updates being made over the internet and instead require an authorisation mechanism that is only available in a clinical setting.

Another key concern is the accessibility of neural implants in case of emergency. Clinicians may be presented with an unconscious or otherwise non-communicative patient whose implant they must access to provide effective treatment, but are unable to do so due to security measures. Thus, the device must have an emergency mode, which leaves open a potential attack vector, meaning that designing such a mode is a technical challenge[27]. Similar considerations must be made with regards to patient programming modes – it is valuable for patients to be able to access their own implants and change stimulation parameters to some degree at home, but allowing too great a degree of control *via* patient programmers enables easy access for attackers or misuse by patients.

Conclusions

Use of implanted neuromodulation is still a relatively new field, but has already had a great impact on the treatment of several severe neurological disorders. The future of this field is highly promising and, contingent on positive outcomes in clinical trials and gradual reductions in hardware cost, it is probable that these devices will only become more popular. This popularity is also contingent on factors such as public acceptance and reliability of implanted neurostimulators, both of which could be substantially negatively impacted by failures in device security.

It bears repeating that this neurosecurity threat is still likely theoretical. We were not able to identify any evidence that the scenarios detailed above have ever been attempted. Nevertheless, we believe that the issues discussed in this paper indicate that brainjacking is a potentially serious threat that warrants serious discussion before any real-world harms occur. As a result of the paucity of work specifically addressing brainjacking, there are several areas of investigation that may prove fruitful.

First, as this review is merely a first step towards more rigorous discussion of neurosecurity issues, there are doubtless several as-yet unidentified potential attack strategies. The focus of the present paper has been on IPGs for DBS but epilepsy monitoring systems, sensory prosthetics, brain-

computer interfaces, and other emerging neurotechnologies are all likely to have device-specific opportunities and challenges worthy of study. Detailed threat modelling may prove to be useful in identification of the most effective strategies for minimising neurosecurity related risk. Stakeholders should collaborate to quantify the expected risk of brainjacking in order to facilitate development of mitigation strategies.

Second, more resources should be put into development of novel mechanisms to enhance neurosecurity, along with appropriation of mechanisms utilised in other fields. It may be valuable to develop codes of best practice for neurosecurity, or to formulate overall guidelines for medical device security that can be tailored to the specific requirements of neural implants. Any such code should be formulated to encourage cooperation between stakeholders and be sufficiently flexible to adapt to the rapid pace of change in neurological implant design. Device manufacturers must strive to improve upon recent advances, ensuring that security concerns are considered throughout the design process and not relegated to an afterthought, and should cooperate with security researchers who seek to responsibly disclose design flaws. Regulatory bodies must balance use of their powers to encourage good neurosecurity practices with the risk of impairing real-world security through overly burdensome regulations. Given that neurosecurity is not an immediate concern, there is sufficient time for manufacturers and regulatory agencies to carefully consider methods of risk mitigation. While there is a responsibility for manufacturers to make their devices secure, the expected value of any novel security features should be carefully weighed against other clinically relevant factors, and innovation should not be unduly stifled by the demands of neurosecurity.

Third, given the unique challenges presented by brainjacking, further research into its implications beyond purely biomedical considerations may be valuable. The philosophical implications of exerting control over another human being in this manner are potentially quite profound and deserving of detailed analysis. Similarly, the legal and economic implications may be substantial, especially if greatly increased proliferation of neurotechnology is to be expected.

Finally, publicising these risks among clinicians and patients may be an important means of minimising risks. Even if it were possible to implement perfect security design, the human element of a system almost always presents a tempting target for attackers. Clinicians should educate themselves about the basics of information security and be mindful of the risks of brainjacking when evaluating faulty implants or caring for high-profile patients. Hospital staff should also be aware of social engineering techniques used by attackers to gain privileged information and should have at least a basic understanding of how to minimise neurosecurity risk. Patients should have some degree of awareness of particularly risky behaviours to avoid, although any discussion of this topic should avoid undue alarm and emphasise the extremely low probability of any individual patient being targeted by electronic attacks.

In writing this paper, we are aware that the information contained herein could be used by an attacker to engage in one of the attacks described above. This is a risk we take seriously, but we believe that the benefits of publicising this topic outweigh the increased danger. The physiological mechanisms that we describe are all easily accessible in scientific journals and any intellectually capable attacker could do their own research; the main challenge for an attacker is in accessing the implanted devices, not in deciding what to do once access is achieved. Furthermore, as discussed above, the current risk of brainjacking is low. The examples given in this paper are intended to illustrate attacks that could be made even with our current, relatively crude, level of neurotechnology. It is better to consider this issue seriously now, rather than in a several years' time when the sophistication of these implants is far greater, as would be the harm that an attacker may cause by subverting them.

The advantages offered by integrating electronics with the human nervous system are substantial and the rapid development of this area suggests even greater things to come in the future. As with many emerging technologies, these advances are not without risks and pitfalls. The histories of both

information security and medicine have amply demonstrated that prevention is better than cure, so let us apply these lessons to neurosecurity while the situation remains relatively tractable.

Funding and acknowledgements

The authors would like to thank the Norman Collisson Foundation and NIHR Oxford Biomedical Research Centre for funding this work. Thanks to B. Cheeran, A. Dwyer, A. Gillespie, H. Maslen, P. Nye, A. Sandberg, and T. Siepmann for feedback and support.

References

1. Gibson W. *Neuromancer*. New York: Ace Books; 1984.

2. Masamune S. Ghost in the Shell. *Wkly Young Mag*. May 1989.

3. Denning T, Matsuoka Y, Kohno T. Neurosecurity: security and privacy for neural devices. *Neurosurg Focus*. 2009;27(1):E7. doi:10.3171/2009.4.FOCUS0985.

4. Shen H. Neuroscience: Tuning the brain. *Nature*. 2014;507(7492):290-292. doi:10.1038/507290a.

5. Lyons MK. Deep brain stimulation: current and future clinical applications. *Mayo Clin Proc*. 2011;86(7):662-672. doi:10.4065/mcp.2011.0045.

6. Hariz M, Blomstedt P, Zrinzo L. Future of brain stimulation: new targets, new indications, new technology. *Mov Disord*. 2013;28(13):1784-1792. doi:10.1002/mds.25665.

7. Hu R, Eskandar E, Williams Z. Role of deep brain stimulation in modulating memory formation and recall. *Neurosurg Focus*. 2009;27(1):E3. doi:10.3171/2009.4.FOCUS0975.

8. Lipsman N, Mendelsohn D, Taira T, Bernstein M. The contemporary practice of psychiatric surgery: results from a survey of North American functional neurosurgeons. *Stereotact Funct Neurosurg*. 2011;89(2):103-110. doi:10.1159/000323545.

9. Bostrom N, Sandberg A. Cognitive Enhancement: Methods, Ethics, Regulatory Challenges. *Sci Eng Ethics*. 2009;15:311-341. doi:10.1007/s11948-009-9142-.

10. Fumagalli M, Priori A. Functional and clinical neuroanatomy of morality. *Brain*. 2012;135(Pt 7):2006-2021. doi:10.1093/brain/awr334.

11. McIntyre CC, Chaturvedi A, Shamir RR, Lempka SF. Engineering the Next Generation of Clinical Deep Brain Stimulation Technology. *Brain Stimul*. 2015;8(1):21-26. doi:10.1016/j.brs.2014.07.039.

12. Radcliffe J. Hacking medical devices for fun and insulin: Breaking the human SCADA system. In: *Black Hat Briefings*. ; 2011.

13. Robertson J. Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device. *Bloomberg.com*. 2012. http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/.

14. Pauli D. Hacked terminals capable of causing pacemaker deaths. *ITnews.com.au*. 2012. http://www.itnews.com.au/News/319508,hacked-terminals-capable-of-causing-pacemaker-mass-murder.aspx.

15. Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In: *2008 IEEE Symposium on Security and Privacy (Sp 2008)*. IEEE; 2008:129-142. doi:10.1109/SP.2008.31.

16. FDA. *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*.; 2013. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

17. FDA. *Collaborative Approaches for Medical Device and Healthcare Cybersecurity*.; 2014. http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM419427.pdf.

18. FDA. Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff. 2016. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

19. FDA. *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*.; 2015. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm. Accessed August 18, 2015.

20. Department of Homeland Security: Industrial control systems cyber emergency response team. Medical Devices Hard-Coded Passwords. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01. Published 2013. Accessed August 24, 2015.

21. Benedict B, Keyes R, Sauls FC. The insulin pump as murder weapon: a case report. *Am J Forensic Med Pathol*. 2004;25(2):159-160. doi:10.1097/01.paf.0000127383.69760.72.

22. Gupta S. Dick Cheney's Heart. CBS. http://www.cbsnews.com/news/dick-cheneys-heart/. Published 2013. Accessed July 25, 2015.

23. Fenoy AJ, Simpson RK. Risks of common complications in deep brain stimulation surgery: management and avoidance. *J Neurosurg*. 2014;120(1):132-139. doi:10.3171/2013.10.JNS131225.

24. Paulson K. Hackers Assault Epilepsy Patients via Computer. Wired. http://archive.wired.com/politics/security/news/2008/03/epilepsy. Published 2008. Accessed September 17, 2015.

25. Gallagher S. Highway to hack: Why we're just at the beginning of the auto-hacking era. Ars Technica. http://arstechnica.com/security/2015/08/highway-to-hack-why-were-just-at-the-beginning-of-the-auto-hacking-era/. Published 2015.

26. I Am the Cavalry. Five Star Automotive Cyber Safety Program. https://www.iamthecavalry.org/domains/automotive/5star/. Published 2014. Accessed August 24, 2015.

27. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey. *J Biomed Inform*. 2015;55:272-289. doi:10.1016/j.jbi.2015.04.007.

28. Park C-S. Security mechanism based on Hospital Authentication Server for secure application of implantable medical devices. *Biomed Res Int*. 2014;2014:543051.

doi:10.1155/2014/543051.

29. Hall JL, McGraw D. For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Aff (Millwood)*. 2014;33(2):216-221. doi:10.1377/hlthaff.2013.0997.

30. Butson CR, Cooper SE, Henderson JM, McIntyre CC. Patient-specific analysis of the volume of tissue activated during deep brain stimulation. *Neuroimage*. 2007;34(2):661-670. doi:10.1016/j.neuroimage.2006.09.034.

31. Morishita T, Foote KD, Burdick AP, et al. Identification and management of deep brain stimulation intra- and postoperative urgencies and emergencies. *Parkinsonism Relat Disord*. 2010;16(3):153-162. doi:10.1016/j.parkreldis.2009.10.003.

32. Shah D, Jimenez Shahed J. Clinical Manifestations of Tolerance to Deep Brain Stimulation (P6.075). *Neurology*. 2014;82(10_Supplement):P6.075 - . http://www.neurology.org/content/82/10_Supplement/P6.075. Accessed September 29, 2015.

33. Vora AK, Ward H, Foote KD, Goodman WK, Okun MS. Rebound symptoms following battery depletion in the NIH OCD DBS cohort: clinical and reimbursement issues. *Brain Stimul*. 2012;5(4):599-604. doi:10.1016/j.brs.2011.10.004.

34. Ooms P, Blankers M, Figee M, et al. Rebound of affective symptoms following acute cessation of deep brain stimulation in obsessive-compulsive disorder. *Brain Stimul*. 7(5):727-731. doi:10.1016/j.brs.2014.06.009.

35. Martin T, Hsiao M, Ha D, Krishnaswami J. Denial-of-Service Attacks on Battery-powered Mobile Computers. March 2004:309. http://dl.acm.org/citation.cfm?id=977406.978701. Accessed August 24, 2015.

36. Burbaud P, Vital A, Rougier A, et al. *Minimal Tissue Damage after Stimulation of the Motor Thalamus in a Case of Chorea-Acanthocytosis.* Neurology 59, 1982-1984 (2002).

doi:10.1212/01.WNL.0000038389.30437.1E.

37. Haberler C, Alesch F, Mazal PR, et al. No tissue damage by chronic deep brain stimulation in Parkinson's disease. *Ann Neurol*. 2000;48(3):372-376. doi:10.1002/1531-8249(200009)48:3<372::AID-ANA12>3.0.CO;2-0.

38. Henderson JM, Pell M, O'Sullivan DJ, et al. Postmortem analysis of bilateral subthalamic electrode implants in Parkinson's disease. *Mov Disord*. 2002;17(1):133-137. doi:10.1002/mds.1261.

39. Yuen TG, Agnew WF, Bullara LA, Jacques S, McCreery DB. Histological evaluation of neural damage from electrical stimulation: considerations for the selection of parameters for clinical application. *Neurosurgery*. 1981;9(3):292-299. http://www.ncbi.nlm.nih.gov/pubmed/7301072. Accessed July 31, 2015.

40. McCreery DB, Agnew WF, Yuen TG, Bullara L. Charge density and charge per phase as cofactors in neural injury induced by electrical stimulation. *IEEE Trans Biomed Eng*. 1990;37(10):996-1001. http://www.ncbi.nlm.nih.gov/pubmed/2249872. Accessed July 31, 2015.

41. Shannon R V. A model of safe levels for electrical stimulation. *IEEE Trans Biomed Eng*. 1992;39(4):424-426. doi:10.1109/10.126616.

42. McIntyre CC, Butson CR, Maks CB, Noecker AM. Optimizing deep brain stimulation parameter selection with detailed models of the electrode-tissue interface. *Conf Proc . Annu Int Conf IEEE Eng Med Biol Soc IEEE Eng Med Biol Soc Annu Conf*. 2006;1:893-895. doi:10.1109/IEMBS.2006.260844.

43. Boccard SG, Fernandes H, Jbabdi S, et al. A tractography study of Deep Brain Stimulation of the Anterior Cingulate Cortex in chronic pain: a key to improve the targeting. *World Neurosurg*. September 2015. doi:10.1016/j.wneu.2015.08.065.

44. Green AL, Aziz TZ. Steering technology for deep brain stimulation. *Brain*. 2014;137(Pt 7):1854-1856. doi:10.1093/brain/awu126.

45. Birdno MJ, Grill WM. Mechanisms of deep brain stimulation in movement disorders as revealed by changes in stimulus frequency. *Neurotherapeutics*. 2008;5(1):14-25. doi:10.1016/j.nurt.2007.10.067.

46. Timmermann K, Wojtecki L, Gross J, et al. Ten-Hertz stimulation of subthalamic nucleus deteriorates motor symptoms in Parkinson's disease. *Mov Disord*. 2004;19(11):1328-1333. doi:10.1002/mds.20198.

47. Fogelson N, Kuhn AA, Silberstein P, et al. Frequency dependent effects of subthalamic nucleus stimulation in Parkinson's disease. *Neurosci Lett*. 2005;382(1-2):5-9.

48. Eusebio A, Chen CC, Lu CS, et al. Effects of low-frequency stimulation of the subthalamic nucleus on movement in Parkinson's disease. *Exp Neurol*. 2008;209(1):125-130. doi:10.1016/j.expneurol.2007.09.007.

49. Rizzone M. Deep brain stimulation of the subthalamic nucleus in Parkinson's disease: effects of variation in stimulation parameters. *J Neurol Neurosurg Psychiatry*. 2001;71(2):215-219. doi:10.1136/jnnp.71.2.215.

50. Krack P, Pollak P, Limousin P, et al. Opposite motor effects of pallidal stimulation in Parkinson's disease. *Ann Neurol*. 1998;43(2):180-192. doi:10.1002/ana.410430208.

51. Kuncel AM, Cooper SE, Wolgamuth BR, et al. Clinical response to varying the stimulus parameters in deep brain stimulation for essential tremor. *Mov Disord*. 2006;21(11):1920-1928. doi:10.1002/mds.21087.

52. Bittar RG, Kar-Purkayastha I, Owen SL, et al. Deep brain stimulation for pain relief: a meta-analysis. *J Clin Neurosci*. 2005;12(5):515-519. doi:10.1016/j.jocn.2004.10.005.

53. Boccard SGJ, Fitzgerald JJ, Pereira EAC, et al. Targeting the affective component of chronic

pain: a case series of deep brain stimulation of the anterior cingulate cortex. *Neurosurgery*. 2014;74(6):628-635; discussion 635-637. doi:10.1227/NEU.0000000000000321.

54. Boccard SGJ, Pereira EAC, Aziz TZ. Deep brain stimulation for chronic pain. *J Clin Neurosci*. June 2015. doi:10.1016/j.jocn.2015.04.005.

55. Pereira EAC, Aziz TZ. Neuropathic pain and deep brain stimulation. *Neurotherapeutics*. 2014;11(3):496-507. doi:10.1007/s13311-014-0278-x.

56. Weintraub D, Siderowf AD, Potenza MN, et al. Association of dopamine agonist use with impulse control disorders in Parkinson disease. *Arch Neurol*. 2006;63(7):969-973. doi:10.1001/archneur.63.7.969.

57. Weintraub D, Koester J, Potenza MN, et al. Impulse control disorders in Parkinson disease: a cross-sectional study of 3090 patients. *Arch Neurol*. 2010;67(5):589-595. doi:10.1001/archneurol.2010.65.

58. Gee L, Smith H, De La Cruz P, et al. The Influence of Bilateral Subthalamic Nucleus Deep Brain Stimulation on Impulsivity and Prepulse Inhibition in Parkinson's Disease Patients. *Stereotact Funct Neurosurg*. 2015;93(4):265-270. doi:10.1159/000381558.

59. Zurowski M, O'Brien JD. Developments in impulse control behaviours of Parkinson's disease. *Curr Opin Neurol*. 2015;28(4):387-392. doi:10.1097/WCO.0000000000000209.

60. Kulisevsky J, Berthier ML, Gironell A, Pascual-Sedano B, Molet J, Parés P. Mania following deep brain stimulation for Parkinson's disease. *Neurology*. 2002;59(9):1421-1424. doi:10.1212/WNL.59.9.1421.

61. Raucher-Chéné D, Charrel C-L, de Maindreville AD, Limosin F. Manic episode with psychotic symptoms in a patient with Parkinson's disease treated by subthalamic nucleus stimulation: improvement on switching the target. *J Neurol Sci*. 2008;273(1-2):116-117. doi:10.1016/j.jns.2008.05.022.

62. Herzog J, Reiff J, Krack P, et al. Manic episode with psychotic symptoms induced by subthalamic nucleus stimulation in a patient with Parkinson's disease. *Mov Disord*. 2003;18(11):1382-1384. doi:10.1002/mds.10530.

63. Smeding HMM, Goudriaan AE, Foncke EMJ, Schuurman PR, Speelman JD, Schmand B. Pathological gambling after bilateral subthalamic nucleus stimulation in Parkinson disease. *J Neurol Neurosurg Psychiatry*. 2007;78(5):517-519. doi:10.1136/jnnp.2006.102061.

64. Wojtecki L, Nickel J, Timmermann L, et al. Pathological crying induced by deep brain stimulation. *Mov Disord*. 2007;22(9):1314-1316. doi:10.1002/mds.21266.

65. Low HL, Sayer FT, Honey CR. Pathological crying caused by high-frequency stimulation in the region of the caudal internal capsule. *Arch Neurol*. 2008;65(2):264-266. doi:10.1001/archneurol.2007.53.

66. Okun MS. Pseudobulbar crying induced by stimulation in the region of the subthalamic nucleus. *J Neurol Neurosurg Psychiatry*. 2004;75(6):921-923. doi:10.1136/jnnp.2003.016485.

67. Krack P, Kumar R, Ardouin C, et al. Mirthful laughter induced by subthalamic nucleus stimulation. *Mov Disord*. 2001;16(5):867-875. doi:10.1002/mds.1174.

68. Wojtecki L, Timmermann L, Groiss SJ, et al. Long-term time course of affective lability after subthalamic deep brain stimulation electrode implantation. *Neurocase*. 2011;17(6):527-532. doi:10.1080/13554794.2010.547507.

69. Okun MS, Mann G, Foote KD, et al. Deep brain stimulation in the internal capsule and nucleus accumbens region: responses observed during active and sham programming. *J Neurol Neurosurg Psychiatry*. 2007;78(3):310-314. doi:10.1136/jnnp.2006.095315.

70. Shapira NA, Okun MS, Wint D, et al. Panic and fear induced by deep brain stimulation. *J Neurol Neurosurg Psychiatry*. 2006;77(3):410-412. doi:10.1136/jnnp.2005.069906.

71. Sousa MB, Reis T, Reis A, Belmonte-de-Abreu P. New-onset panic attacks after deep brain

stimulation of the nucleus accumbens in a patient with refractory obsessive-compulsive and bipolar disorders: a case report. *Rev Bras Psiquiatr*. 37(2):182-183. doi:10.1590/1516-4446-2014-1581.

72. HEATH RG. ELECTRICAL SELF-STIMULATION OF THE BRAIN IN MAN. *Am J Psychiatry*. 1963;120:571-577. http://www.ncbi.nlm.nih.gov/pubmed/14086435. Accessed September 17, 2015.

73. van Kuyck K, Gabriëls LA, Cosyns PR, et al. Behavioural and physiological effects of electrical stimulation in the nucleus accumbens: A review. *Acta Neurochir Suppl*. 2007;97(Pt 2):375-391. doi:10.1007/978-3-211-33081-4-43.

74. Delaloye S, Holtzheimer PE. Deep brain stimulation in the treatment of depression. *Dialogues Clin Neurosci*. 2014;16(1):83-91. http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3984894&tool=pmcentrez&rendertype=abstract. Accessed September 18, 2015.

75. Kocabicak E, Temel Y, Höllig A, Falkenburger B, Tan SK. Current perspectives on deep brain stimulation for severe neurological and psychiatric disorders. *Neuropsychiatr Dis Treat*. 2015;11:1051-1066. doi:10.2147/NDT.S46583.

76. Park RJ, Godier LR, Cowdrey FA. Hungry for reward: How can neuroscience inform the development of treatment for Anorexia Nervosa? *Behav Res Ther*. 2014;62:47-59. doi:10.1016/j.brat.2014.07.007.

77. Raghunathan A, Jha NK. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: *2011 IEEE 13th International Conference on E-Health Networking, Applications and Services*. IEEE; 2011:150-156. doi:10.1109/HEALTH.2011.6026732.

78. Zhang M, Raghunathan A, Jha NK. Trustworthiness of Medical Devices and Body Area Networks. *Proc IEEE*. 2014;102(8):1174-1188. doi:10.1109/JPROC.2014.2322103.

79. Burleson W, Clark SS, Ransford B, Fu K. Design challenges for secure implantable medical devices. In: *Proceedings of the 49th Annual Design Automation Conference on - DAC '12*. ; 2012:12. doi:10.1145/2228360.2228364.

80. Doctorow C, McSherry C. Comments of Electronic Frontier Foundation. Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff. https://www.eff.org/files/2016/04/22/electronic_frontier_foundation_comments_cybersecurity_in_medical_devices_.pdf. Published 2016. Accessed May 3, 2016.

81. Rhew H-G, Jeong J, Fredenburg JA, Dodani S, Patil P, Flynn MP. A wirelessly powered log-based closed-loop deep brain stimulation SoC with two-way wireless telemetry for treatment of neurological disorders. In: *2012 Symposium on VLSI Circuits (VLSIC)*. IEEE; 2012:70-71. doi:10.1109/VLSIC.2012.6243794.

82. Grahn PJ, Mallory GW, Khurram OU, et al. A neurochemical closed-loop controller for deep brain stimulation: toward individualized smart neuromodulation therapies. *Front Neurosci*. 2014;8:169. doi:10.3389/fnins.2014.00169.

83. Kushner D. The Real Story of Stuxnet. IEEE Spectrum. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Published 2013. Accessed May 2, 2016.

84. Hansen JA, Hansen NM. 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 - SPIMACS '10*. New York, New York, USA: ACM Press; 2010:13. doi:10.1145/1866914.1866917.

85. Li C, Raghunathan A, Jha NK. Improving the Trustworthiness of Medical Device Software with Formal Verification Methods. *IEEE Embed Syst Lett*. 2013;5(3):50-53. doi:10.1109/LES.2013.2276434.

86. Rasmussen KB, Castelluccia C, Heydt-Benjamin TS, Capkun S. Proximity-based access control for implantable medical devices. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security - CCS '09*. New York, New York, USA: ACM Press; 2009:410. doi:10.1145/1653662.1653712.

87. Kim Y, Lee WS, Raghunathan V, Jha NK, Raghunathan A. Vibration-based secure side channel for medical devices. In: *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*. New York, New York, USA: ACM Press; 2015:1-6. doi:10.1145/2744769.2744928.

88. Denning T, Fu K, Kohno T. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In: *HotSec*. ; 2008.

89. Gollakota S, Hassanieh H, Ransford B, Katabi D, Fu K. They can hear your heartbeats: non-invasive security for implantable medical devices. *Proc ACM SIGCOMM 2011 Conf SIGCOMM*. 2011:2-13. doi:10.1145/2018436.2018438.

90. Stewart CDM, Eljamel S. Prediction of implantable pulse generator longevity in deep brain stimulation: limitations and possible solutions in clinical practice. *Stereotact Funct Neurosurg*. 2011;89(5):299-304. doi:10.1159/000329360.

91. Little S, Pogosyan A, Neal S, et al. Adaptive deep brain stimulation in advanced Parkinson disease. *Ann Neurol*. 2013;74(3):449-457.

92. Kraemer S, Carayon P, Clem J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Comput Secur*. 2009;28(7):509-520. doi:10.1016/j.cose.2009.04.006.

93. Stone R, McCloy R. Ergonomics in medicine and surgery. *BMJ*. 2004;328(7448):1115-1118. doi:10.1136/bmj.328.7448.1115.

94. Independent Security Evaluators. Securing Hospitals A Research Study and Blueprint. https://securityevaluators.com/hospitalhack/securing_hospitals.pdf. Published 2016.

Accessed May 2, 2016.

95. Kim Y, Lee W, Raghunathan A, Raghunathan V, Jha NK. *Implantable Biomedical Microsystems*. Elsevier; 2015. doi:10.1016/B978-0-323-26208-8.00008-X.

Table 1: Summary of attack types

Attack category	Attack type	Condition	Potential harms
Blind	Switching off IPG	Any	Denial of stimulation; rebound effects
	Draining battery		Denial of stimulation; rebound effects; IPG damage
	Overcharge stimulation		Tissue damage
	Data theft		Violation of patient privacy; facilitation of further attacks
Targeted	~10Hz STN stimulation	PD	Hypokinesia/akinesia
	GPi electrode contact change	PD	
	Increase voltage/decrease frequency ViM stimulation	ET	Exacerbated tremor
	Increased frequency PAG/PVG stimulation	Pain	Increased pain
	Increased frequency VPL/VPM stimulation	Pain	
	STN electrode contact change	PD	Impulse control disoders; alteration of affect
	NAcc electrode contact change	OCD	Alteration of affect
	NAcc stimulation control	OCD, depression	Alteration of reward processing; operant conditioning

Abbreviations: ET, essential tremor; GPi, internal globus pallidus; IPG, implantable pulse generator; NAcc, nucleus accumbens; OCD, obsessive-compulsive disorder; PAG/PVG, periaqueductal/periventricular grey matter; PD, Parkinson's disease; STN, subthalamic nucleus; ViM, ventral intermediate thalamic nucleus; VPL/VPM, ventroposterior lateral/medial thalamic nucleus

Abbreviation list

DBS = Deep Brain Stimulation

ET = Essential Tremor

GPi = internal Globus Pallidus

ICD = Impulse Control Disorder

IPG = Implantable Pulse Generator

NAcc = Nucleus Accumbens

OCD = Obsessive-Compulsive Disorder

PAG = Periaqueductal Grey matter

PVG = Periventricular Grey matter

PD = Parkinson's Disease

STN = Subthalamic Nucleus

VPL = Ventroposterior Lateral thalamic nucleus

VPM = Ventroposterior Medial thalamic nucleus

VTA = Volume of Tissue Activated

Disclosure – conflict of interest

As corresponding author I, Laurie Pycroft, am not aware of any conflicts of interest among any of the authors relevant to this review article.