Hacking Minds, Hacking Brains, Hacking Augmented Bodies: Ethical Aspects of Neurohacking

Marcello Ienca (University of Basel)

Abstract

Emerging trends in pervasive neurotechnology and robotics are rapidly enabling novel opportunities for human-machine interaction and reshaping the human cognitive ecosystem. Clinical applications of neurotechnology such as brain-computer interfaces (BCIs), neuroprosthetics and wearable robotics enable to restore cognitive or motor function in patients with neurological disorders as well as to enhance their interaction with the world.

While these trends can provide immense benefit for neurology and neurorehabilitation, they also open breaches for privacy and security of neural information[1-3]. The more the human body becomes intertwined with digital technology, the more it becomes vulnerable to cyber-risk.

Recent findings have shown that assistive neurodevices can be potentially co-opted for malicious activities such as extracting concealed private information from users without their consent[4-6], cracking encrypted repositories of neural recordings[7] or even interfering with the device's functionality[8]. These findings open the prospects of extending the range of computer-hacking to neural computation.

This emerging domain of brain-machine interaction can be labeled *neurohacking* since it encompasses hacking activities which (either directly or indirectly) target neural information[9]. In this contribution, we identify three different types of neurohacking based on their level of penetration into neural computation. In addition, we distinguish malicious forms of neurohacking –characterized by the unauthorized misuse of neurodevices by malevolent actors- from what we call *ethical neurohacking* –characterized by the open and collaborative development of new neurotechnologies for the benefit of users.

After reviewing a number of experimental and real-world case studies, we delineate the normative and conceptual implications of neurohacking. At the normative ethical level, we address the issues of neuroprivacy, neurosecurity, self-monitoring and de-anonymization raised by emerging trends in neurohacking. Concurrently, at the conceptual level, we explore the implications of neurohacking on critical neurophilosophical notions such as brain-reading, mental content, embodiement and extended cognition.

References

Dupont, B. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review* **3**, 6 (2013).

Eaton, M. L. & Illes, J. Commercializing cognitive neurotechnology--the ethical terrain. *Nat. Biotechnol.* **25**, 393 (2007).

Bonaci, T., Herron, J., Matlack, C. & Chizeck, H. J. Securing the Exocortex: A Twenty-First Century Cybernetics Challenge. *IEEE Technology and Society Magazine* **34**, 44-51 (2015).

Martinovic, I. *et al.* in *USENIX Security Symposium.* 143-158.

Ienca, M. & Haselager, P. Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology* **18**, 117-129 (2016).

Bonaci, T., Calo, R. & Chizeck, H. J. App stores for the brain: Privacy and security in brain-computer interfaces. *IEEE Technology and Society Magazine* **34**, 32-39 (2015).
Conner, M. Hacking the brain: Brain-to-computer interface hardware moves from the realm of research. *EDN* **55**, 30-35 (2010).
Pycroft, L. *et al.* Brainjacking: Implant Security Issues in Invasive Neuromodulation. *World Neurosurg.* **92**, 454-462 (2016).
Denning, T., Matsuoka, Y. & Kohno, T. Neurosecurity: security and privacy for neural devices. *Neurosurg. Focus* **27**, E7 (2009).