Cambridge Quarterly of Healthcare Ethics (2021), 30: 4, 662–668
doi:10.1017/S096318012100013X

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Cyberbiosecurity: An Emerging Field that has Ethical Implications for Clinical Neuroscience

Dov Greenbaum*

Department of Molecular Biophysics and Biochemistry, Yale University New Haven, Connecticut, USA
Harry Radzyner Law School, Interdisciplinary Center, Herzliya, Israel
Zvi Meitar Institute for Legal Implications of Emerging Technologies, IDC, Israel
*Corresponding author: Email: dov.greenbaum@yale.edu

Abstract

Cyberbiosecurity is an emerging field that relates to the intersection of cybersecurity and the clinical and research practice in the biosciences. Beyond the concerns that usually arise in the areas of genomics, this paper highlights ethical concerns raised by cyberbiosecurity in clinical neuroscience. These concerns relate not only to the privacy of the data collected by imaging devices, but also the concern that patients using various stimulatory devices can be harmed by a hacker who either obfuscates the outputs or who interferes with the stimulatory process. The paper offers some suggestions as to how to rectify these increasingly dire concerns.

Keywords: cyberbiosecurity; clinical neuroscience; imaging devices; privacy of data collection

Introduction

Cyberbiosecurity/biocybersecurity is an emerging area of research focusing on the intersection between cybersecurity and the growing bioeconomy. The field emerged as the frontiers of biology and cybersecurity began to collide. There is an increasing biological presence in the cybersecurity field, including the use of biometric data to access computing devices, and the use of biological principles in cybersecurity, such as employing concepts from DNA sequencing in the detection of malware.[1,2]

There is also an increasing cybersecurity presence in the biomedical world. In most cases, the concerns relate to either the growing digitization of biomedical data and the concomitant potential disclosure of patient health records,[3] or synthetic biology and the use and abuse of DNA sequencing technologies to surreptitiously and maliciously introduce problematic DNA sequences in naïve laboratories through hacking various computer systems.[4]

Although there are also overlapping areas in the fields of neuroscience and genetics that raise problematic cyberbiosecurity concerns, such as the malicious manipulation of genes within modified stem cells in the treatment of traumatic brain injury or ischemic stroke,[5] the heretofore focus principally on genetics is an admittedly narrow view of the potential concerns of cyberbiosecurity.

Neuroscience, like genetics, also has an increasing need for cybersecurity. These cyberbiosecurity concerns in the field of clinical neuroscience create ethical concerns principally via the access to or deletion of private healthcare data. Other ethical concerns relate to the inability to provide health services when a neuroscience facility is subject to a cyberattack, especially in poorer hospitals that might be unable to afford advanced cybersecurity technicians, or afford newer more secure devices. Further ethical concerns relate to the misdiagnoses of neurological diseases when neuro-devices have been hacked to present incorrect information. Here again, it is the poorer and/or minority demographics that are most likely to be affected by such situations as there may not be an opportunity for additional medical testing to verify a diagnosis that was based on false information.

We will review some of the concerns as they relate to the current state of the art technologies such as internet enabled neuro-devices in hospitals that open up the medical infrastructure to cyberattacks, emerging technologies, such as brain computer interfaces (BCIs) and Elon Musk's Neuralink, and the future neuroscience technologies.

Cyberbiosecurity

Cyberbiosecurity or Biocybersecurity is a field that is so young it does not even yet have a consistent name. It broadly relates to any or all areas where either bioscience research or clinical activities come in contact with the flow of information over the internet. Consider the two following examples to explain some of the concerns and considerations in cyberbiosecurity.

A mischievous hacker Alice employs software to access the computer of Bob, the naïve bioscientist who might, at most, employ standard password protections on his lab's network and its computers. Bob submits an order to a third party genetic sequencing company, Charlie, to manufacture a particular nonmalicious strand of DNA for an experiment. Alice—who has accessed Bob's computers through perhaps a standard malware or phishing attack, or even guessed Bob's passwords—intercepts Bob's outgoing email to Charlie with the requested strand and changes the order to a malicious strand of DNA. Fortunately, universally accepted standard operating procedures (albeit, somewhat lacking) will require Charlie to inspect the requested strand of DNA for known blacklisted genes that might be dangerous. Unfortunately, Alice can employ standard cyber-hacking tools to design a malicious strand of DNA that seems innocuous and will not be detected by those standard operating procedures. Charlie prints millions of the requested DNA strand and sends them back to Bob, who remains unaware that the DNA is not what he ordered. Bob uses the DNA in his experiments. Ultimately, that DNA causes trouble, either ruining the experiment, or potentially even worse if the resulting protein had toxic properties. Although seemingly an unlikely scenario, a proof of concept experiment was able to accomplish that exact scenario.[6]

In a second scenario, Alice, our hacker, publishes online tools for biologists to use, particularly bioinformaticians. Bob, again our naive scientist at a large pharmaceutical company, might, in searching for a particular tool for creating a precise strand of DNA for future research, uses Alice's tool to design and order the desired strand of DNA. Alice, unbeknownst to Bob, has maliciously designed her tool such that while the output of the tool seems innocuous, the tool itself can be used to hack into Bob's computer, exposing valuable unpublished intellectual property and business information.[7]

The concerns of cyberbiosecuirty, however, go beyond these examples. As additional weaknesses are discovered and manipulated by others like Alice, the scope of the field will expand and grow in importance in genomics, synthetic biology, and clinical neuroscience.

Hospital Neuro-Devices

Hospitals have long been targets of cyberattacks such as ransomware.[8] These are nontrivial as they can end up costing institutions millions of dollars, and possibly even result in the loss and erasure of valuable patient records.[9] This is arguably due to the value of the data housed in hospitals, the inherent privacy of the data, the need to have constant access to the data, and the risk averse nature of these institutions. In addition, hospitals have many internet of things (IoT) medical devices (MDIoT) from varied manufacturers scattered throughout the campus, each one needing to access the hospital's central intranet, and, as such, each one a potential access point for a hacker.[10] These devices are notorious for being unprotected against hackers.[11]

Included within these devices are the many imaging and recording neuro-devices for electroencephalograms, magnetic resonance imaging, positron emission tomography, computerized tomography, magnetoencephalography, as well as the various stimulatory devices that provide transcranial magnetic stimulation, transcranial direct or current stimulation, as well as other neurostimiluators, and neurosurgery devices and robots.

The worldwide market of just the monitoring devices is valued at over 6 billion USD annually within the greater 10 billion USD neurology market[12]; much of that market includes the aforementioned devices supplied by numerous key players. Inconsistencies between the nonstandardized interfaces and idiosyncrasies amongst the many devices means that maintaining optimal security settings for all devices is nearly impossible for the hospital informational technology staff. As such, many of these devices will ultimately be hackable and the resulting private patient data accessible to malicious actors. The ability to hack the system also allows the data to become corrupted either through deletions of valuable information or the addition of confounding information, false data or just noise. Such data could result in the wrong diagnosis and/or wrong prescription which could be harmful to the patient. The data can also be used to assess and target determinable behavior patterns for manipulation and social exploitation.[13]

One example: Implantable pulse generators are regulated devices that are provided to treat conditions such as depression or Parkinson's. These devices are often Bluetooth enabled and allow data to be transferred to software on devices like phones and tablets to manage the generators. Although security experts have yet to see any actual hacks implemented on these devices, they warn that weak encryption, or lack any of encryption, as well as weak passwords, could potentially allow malicious hackers access.[14] If and when these devices are hacked, they could be actively manipulated or mis-calibrated to cause actual physical harm, or even lethality to a patient.

Brain Computer Interfaces

Research exploring the merging of man and machine via brain machine interfaces, or BCIs (brain computer interfaces) has been advancing for decades.[15] The various iterations of the technologies can allow for multi-directional communication between the brain and one or more devices by way of software and hardware. The technology has long raised ethical concerns related to a myriad of issues ranging from questioning free-will to human enhancement.[16,17,18]

However, BCIs can also raise additional ethical concerns as they become subject to biocybersecurity threats. Although current technology does not easily allow for decoding and assigning meaning to the electrical impulses collected by these machines, especially out of context, there are efforts that aim to enable tools like artificial intelligence (AI) to decode the information, even extracting passable images from the signals received from the brain.[19] Those signals, if intercepted could become privacy concerns for the individual who generated them, even being used to infer cognitive abilities and personality traits of the users.[20] Data from BCIs can reflect on the user's physical health, cognition, and mental health.[21] Those signals could also be used to access things that are unlocked via emerging brainwave biometrics.[22,23] The data can also be employed to understand the decision making processes of individuals; such an understanding, if misappropriated could be employed and exploited to that individual's detriment.

BCIs provide additional concerns given their extensive usage in a multitude of different settings, each setting creating their own biocybersecurity concerns. They are used professionally in clinical care, in neuroscience research, and even in the home for both medical and recreational uses[24]. Regardless of the setting of its use, however, there is a need to provide cyber protection for each element of the process connecting the human mind to a machine. These processes at risk include signal acquisition from the brain, preprocessing of the signal, extraction of features from the signal, classification and translation of the signal, and even user feedback after examining the output.

The risks of ethical concerns are exacerbated by the reality that the data are often not encrypted as they pass between various software and hardware devices—sometimes wired, and sometimes wirelessly—opening up the system to increasing threats. Even if the mostly unintelligible data within these devices does not impinge on the ultimate privacy of the individual, as per current conventional wisdom, the data are still per se the property of the user, and the taking of the data could be an ethical, if not legal misappropriation of the user's property.

In general, the hacking of these systems can have repercussions regarding the integrity and usability of the device, data can be altered both incoming and outgoing, artificial information or noise can be added, and privacy of the user's data can be impinged. Even the ultimate safety of the user and those around her[25]: BCIs are often attached to devices such as prosthetics[26] and rehabilitative exoskeletons.[27] If the interface becomes compromised via a hack, either through inserted malicious code, or over the air via unsecured wireless transmission between the BCI and the device, a hacker could take control of the device, even committing a crime. It would be difficult to prove that the crime was committed by a hack and not by the owner of the prosthetic.[28]

Not only are the hardware devices often problematic vis-à-vis cyber protection, but the underlying software is often opensource and potentially untrustworthy. That code can create further concerns. Increasingly, BCIs are incorporating AI into the analysis of the harvested neural signals. The complexity of AI, especially the somewhat opacity of AI decisions, and their sometimes-unexpected results, provide additional opportunities for hackers to conceal malicious code within the BCI software. That malicious code could hijack, change, or obfuscate the neural signals collected by the BCIs.

Neuralink

Elon Musk's much hyped Neuralink device is supposed to be user friendly as well as medically relevant.[29] The device is effectively unique in comparison to the current state of the art, as an implanted brain machine interface with potentially thousands of individual connections to neurons. The device is supposed to incorporate both a standard USB interface as well as wireless (Bluetooth) capabilities.[30] Given the very public nature of the device and the potential and unknowable repercussions for being hacked, the device will likely be a very attractive target for hackers who could cause real damage via, say, overstimulation of the brain via the device.

These threats of cyberattacks are further raised as the device is intended to be compatible with smartphone devices and their onboard third-party apps and potentially also store data in the cloud. A relatively novel ethical concern with Neuralink compared to other devices in clinical neuroscience is the degree to which the device will be communicating with the internet and the consent that such communication will demand. Given the degree of access that Neuralink will have to a user's brain, effectively 24/7, Neuralink will need to be constantly implementing software patches to maintain security. Those patches will likely need to be implemented without user consent, given their dire necessity, as well as the likelihood that some users will be unable, unwilling, or underwhelmed to implement those patches on their own. This lack of consent is ethically problematic.

Further, given its stated expected ability to interact with standard computing interfaces, if Neuralink becomes employed as a biometric device, hacking Neuralink will allow hackers to access other systems and networks that employ Neuralink for authentication. Even the implantation of the Neuralink device via a robot that drills through a patient's skull to access her brain raises cybersecurity concerns. Even small errors in that area can have monumental repercussions.

The Role of Cyberbiosecurity

The latter examples are just a few of the many areas where clinical neuroscience may have to consider the emerging repercussions of cyberbiosecurity concerns. As technology continues to advance and more records are maintained online, in the cloud, or connected tablets and devices, all being fed by internet enabled neuro IoT devices, both in professional as well as recreational settings, those concerns will only continue to grow. The images recorded of our brains during daily or specialized activities, or recordings of electrical impulses go to the very essence of who we are as a person. It is vital that these data points are protected from both random and directed malicious hacks. Regardless as to whether that data are actually usably discernable today, or sometime in the near future, the data ought to be safeguarded. It is

the ethical responsibility of manufactures, regulators, and practitioners to make sure that the data are safe and secure.

Within this world, the nascent field of cyberbiosecurity, which grew out of the older biosecurity field,[31] has a number of important roles. Researchers from diverse disciplines in computer science, counterterrorism, cybersecurity, neuroscience, genomics, synthetic biology, policy, and law are all coalescing to create and maintain this field.[32]

These researches need to threat-model the concerns and map out the various potential weaknesses in typical clinical and research centers, protocols, and commonly used hardware and software tools. Each of these areas could potentially provide gaping holes for hackers and other actors to access information or technologies. This is nontrivial, and in some instances, can involve brute forcing multiple different simulations on various pieces of clinical neuroscience infrastructure to assess what is benign and what is potentially dangerous.

The field must also act to devise countermeasures that can be employed to prevent such attacks, including planning and applying standards of cybersecurity, and working to have software patched where it can be. Efforts should be made especially in poorer areas to assist in updating and securing these devices. Further, like cybersecurity command centers, cyberbiosecurity needs professionals to monitor emerging hacks and targets, and provide accurate assessments to the field.

The field will be further helped by the development of outreach and educational efforts that seek to inform the clinicians and researchers in neuroscience as to the potential dangers and pitfalls that can occur at the intersection of computing devices, the internet of things, and neuroscience. Especially, but not always, in laboratories and hospital settings. The continued publication of papers, like this one, will help inculcate practitioners as to the potential dangers lurking behind their internet routers.

Ultimately, the field should work toward systems of institutional self-governance that appreciate the need to include cybersecurity in business operations considerations and risk management, and/or expanded regulatory oversight for medical devices. With clear regulations, the field can then push manufactures of relevant devices and software to engineer their products through incorparating ethics-by-design and privacy- by -design, such that features like two-factor identification, end-to-end encryption, and other aspects of cybersecurity and privacy protection are incorporated into products as the default.

Conclusions

Many in the clinical neuroscience field may not yet be knowledgeable as to the extent that cyberbiosecurity or biocybersecurity plays, or will play, in their research. The goal of this short overview of the field is to rectify that perception. Failure to consider the ramifications resulting from the lack of proper protocols, expansive oversight and regulation, standardization, and general good practices could create both ethical and legal problems for practitioners in the field of clinical neuroscience.

Notes

1. Khan F, Ncube C, Ramasamy LK, Kadry S, Nam Y. A digital DNA sequencing engine for ransomware detection using machine learning. *IEEE Access* 2020;**8**:119710–9.
2. Dinh A, Brill D, Li Y, He W. Malware sequence alignment. In *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)(BDCloud-SocialCom-SustainCom)*; 2016 (pp. 613–7). IEEE.
3. Berger KM, Roderick J. *National and Transnational Security Implications of Big Data in the Life Sciences*. New York, NY: American Association for the Advancement of Science; 2014.
4. Puzis R, Farbiash D, Brodt O, Elovici Y, Greenbaum, D. Increased cyber-biosecurity for DNA synthesis. *Nature Biotechnology* 2020;**38**(12):1379–81.

5. Shahror RA, Wu CC, Chiang YH, Chen KY. Genetically modified mesenchymal stem cells: The next generation of stem cell-based therapy for TBI. *International Journal of Molecular Sciences* 2020;**21** (11):4051.
6. Farbiash D, Puzis R. Cyberbiosecurity: DNA injection attack in synthetic biology. 2020. *arXiv preprint arXiv:2011.14224.*
7. Murch R. Security vulnerabilities in the bioeconomy existed prior to synthetic biology. *Presentation to the NAS National Materials and Manufacturing Board*, May 1, 2019.
8. Spence N, Bhardwaj N Paul, III DP. Ransomware in healthcare facilities: A Harbinger of the future? *Perspectives in Health Information Management* 2018;1–22.
9. Ibarra J, Jahankhani H, Kendzierskyj S. Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime. In: *Blockchain and Clinical Trial*. Cham: Springer; 2019, at 115–37.
10. Greenbaum D. Avoiding overregulation in the medical internet of things. In: Cohen IG, Fernandez Lynch H, Vayena E, Gasser U, eds. *Big Data, Health Law, and Bioethics*. Cambridge: Cambridge University Press; 2018:129–41.
11. Newman LH. *A new pacemaker hack puts malware directly on the device. Wired*; August 9, 2018; available at https://www.wired.com/story/pacemaker-hack-malware-black-hat/ (accessed 20 Jan 2021).
12. https://www.marketsandmarkets.com/Market-Reports/brain-monitoring-devices-market-909.html#:~:text=brain%20monitoring%20market%3F-,The%20global%20brain%20monitoring%20market%20size%20is%20estimated%20to%20be,in%20the%20Brain%20Monitoring%20market%3F
13. DeFranco J, DiEuliis D, Giordano J. Redefining neuroweapons. *PRISM* 2019;**8**(3):48–3.
14. Scammell R. Brain hacking: Will our memories be safe? *Verdict*; Oct 30 2018; available at https://www.verdict.co.uk/brain-hacking-memories-safe/?utm_source=Army%20Technology&utm_medium=website&utm_campaign=Must%20Read&utm_content=Image (accessed 10 June 2021)
15. Abiri R, Borhani S, Sellers EW, Jiang Y, Zhao X. A comprehensive review of EEG-based brain–computer interface paradigms. *Journal of Neural Engineering* 2019;**16**(1):011001.
16. Nakar S, Weinberger S, Greenbaum D. Legal and social implications of predictive brain machine interfaces: Duty of care, negligence, and criminal responsibility. *American Journal of Bioethics, Neuroscience* 2015;**6**(4):40–2.
17. Dadia T, Greenbaum D. Neuralink: The ethical 'rithmatic of reading and writing to the brain. *American Journal of Bioethics Neuroscience* 2019;**10**(4):187–9.
18. Coin A, Dubljević V. The authenticity of machine-augmented human intelligence: Therapy, enhancement, and the extended mind. *Neuroethics* 2020;1–8.
19. Rashkov GV, Bobe AS, Fastovets DV, Komarova MV. Natural image reconstruction from brain waves: A novel visual BCI system with native feedback. *bioRxiv*, 2019;787101.
20. Landau O, Cohen A, Gordon S, Nissim N. Mind your privacy: Privacy leakage through BCI applications using machine learning methods. *Knowledge-Based Systems* 2020 **198**;105932.
21. Greenberg A. Inside the mind's eye: An international perspective on data privacy law in the age of brain machine interfaces. *Albany Law Journal of Science & Technology* 2019;**29**:79.
22. Blondet MVR, Laszlo S, Jin Z.. Assessment of permanence of non-volitional EEG brainwaves as a biometric. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*; 2015, at 1–6.
23. Bansod NS, Dabhade SB, Kazi MM, Rode YS, Kale KV. Single electrode brain signal data fusion for security. In *2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*; 2016, at 108–12.
24. Blankertz B, Tangermann M, Vidaurre C, Fazli S, Sannelli C, Haufe S, *et al.* The Berlin brain–computer interface: Non-medical uses of BCI technology. *Frontiers in Neuroscience* 2010;**4**:198.
25. Belkacem AN. Cybersecurity framework for P300-based brain computer interface. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*; 2020, at 1–6.

26. Andersen RA, Aflalo T, Kellis S. From thought to action: The brain–machine interface in posterior parietal cortex. *Proceedings of the National Academy of Sciences* 2019;**116**(52):26274–9.
27. Benabid AL, Costecalde T, Eliseyev A, Charvet G, Verney A, Karakas S, *et al.* An exoskeleton controlled by an epidural wireless brain–machine interface in a tetraplegic patient: a proof-of-concept demonstration. *The Lancet Neurology* 2019;**18**(12):1112–22.
28. Greenbaum D. Ethical, legal and social concerns relating to exoskeletons. *ACM SIGCAS Computers and Society*. 2016 Jan 5;**45**(3):234–9.
29. Musk E. An integrated brain-machine interface platform with thousands of channels. *Journal of Medical Internet Research* 2019;**21**(10):e16194.
30. Lewis T. *Elon Musk's pig-brain implant is still a long way from 'solving paralysis.' Scientific American*; September 2, 2020; available at https://www.scientificamerican.com/article/elon-musks-pig-brain-implant-is-still-a-long-way-from-solving-paralysis/ (accessed 20 Jan 2021).
31. Gillum D, Carrera LAO, Mendoza IA, Bates P, Bowens D, Jetson Z. *et al.* The 2017 Arizona biosecurity workshop: An open dialogue about biosecurity. *Applied Biosafety* 2018;**23**(4):233–41.
32. Murch RS, So WK, Buchholz WG, Raman S, Peccoud J. Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology* 2018;**6**:39.

Cite this article: Greenbaum, D. 2021. Cyberbiosecurity: An Emerging Field that has Ethical Implications for Clinical Neuroscience. *Cambridge Quarterly of Healthcare Ethics* 30: 662–668, doi:10.1017/S096318012100013X