Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 57 – 63 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

NEUROETHICAL QUANDARIES AT THE CROSSROADS OF CYBERSPACE

Er. Ms. Kritika[1]

[1] Independent Researcher, India

ABSTRACT: The booming landscape of multidisciplinary studies, namely, neuroscience, ethics and cyber security brings into focus the emerging need of developing ethical standards for neural data to the implemented safely in the domain of cyberspace. The synergy between neuroscience and cybersecurity emphasizes the transformative potential of technologies like BCI, EEG, FMRI, MEG etc. highlighting the ethical imperative to bring to light the issues of privacy, autonomy, individual's right, and security of their neural data. The paper delves into the question of delicacy of neuro data as an emerging concern for cyber professionals as well as individuals to safeguard from the emerging threats of phishing, brain jacking, vishing and implementing proper guidelines and framework to have informed consent before going ahead with their confidential data which can otherwise be misused at the hands of cybercriminals.

KEYWORDS: Neuroethics, Cybersecurity, Neuroimaging Technologies, BCI

1. INTRODUCTION

A novel approach that acknowledges the weaknesses in the modern human mind and seeks to strengthen defence against cyberattacks is the integration of neuroscience with cybersecurity. Due to social engineering, phishing, and other strategies that take advantage of people's cognitive abilities and make them unintentionally complicit in security breaches, this convergence acknowledges the human aspect as a major role in cyber dangers. Cybersecurity systems [3] can be built to identify abnormalities in user behaviour by comprehending the cognitive processes connected to deceit, stress, or malevolent intent with an extra line of defence against insider threats and complex attacks can be added by integrating neurobiological markers, such as physiological reactions, eye movement patterns, or cognitive strain, into advanced threat detection algorithms. Biometric markers might be, for example, an individual's physiological reactions, tracked by wearable technology or specialized sensors. Traditional behavioural analytics is strengthened and made more resilient to new threats by this neuroscience-informed method. Another area where neuroscience might improve security through individual cognitive variables is in cognitive authentication and access control. Based on brainwave patterns or the cognitive reaction to particular stimuli, neuro-authentication may offer a more safe and dependable way to confirm user identification. Developments in Brain-Computer Interfaces (BCIs) [36, 37] provide a possible path towards cognitive authentication implementation. Organizations may strengthen security by providing an extra layer of authentication beyond conventional techniques by integrating these cognitive biometrics into access control systems.

As neuroscience and cybersecurity grow increasingly integrated, safeguarding cognitive privacy becomes a critical ethical concern. The gathering and examination of brain data gives rise to worries regarding possible abuse or unapproved access to people's feelings and thoughts. Establishing ethical frameworks is necessary to guarantee that neuro-cybersecurity measures respective individual autonomy and privacy rights. Programmes for human-centered awareness and training can also profit from neuroscience by learning about people's perceptions and processing of security-related information might help designers create training modules that are more successful that are based on cognitive science concepts, neuroeducation can improve users' ability to remember and apply cybersecurity best practices.

Organizations may enable users to identify possible hazards and take appropriate action more efficiently by customizing training programmes to correspond with cognitive processes. Another way that neuroscience may help design adaptable cybersecurity systems that learn and adjust based on real-time assessments of user behaviour and environmental conditions is through neuro-inspired adaptability. Algorithms with artificial intelligence have the potential to imitate the human mind's capacity for adaptation and learning, allowing them to continually update their comprehension of typical user behaviour and spot abnormalities.

The rapid progress in brain research and technological advancements has led to an increased interest in the multidisciplinary topic of neuro-ethics, a blend of neuroscience and ethics. Ethical issues gain importance as our knowledge of the brain increases and applications in neuroscience grow with the goal to discuss the moral ramifications of comprehending, modifying, and controlling the brain with the subjects including personhood, consciousness, brain-computer interfacing, and cognitive augmentation. As concerns regarding cognitive privacy, the right to govern ideas, and potential unintended implications on human identity grow, respect for autonomy is a basic ethical tenet. The transdisciplinary field of neuro-ethics studies the philosophical, legal, and social ramifications of neuroscience investigating the cultural presumptions on identity, consciousness, cognitive experience, and decision-making [1]. It involves different elements of research ethics, including informed consent, privacy and confidentiality, clinical applications, medical interventions, legal and societal ramifications, education, dual-use technology, and philosophical and conceptual difficulties which includes [2] obtaining participants' informed consent, handling sensitive brain data collection and storage issues, and discussing the moral implications of medical interventions such as deep brain stimulation and brain imaging, as well as neuro enhancement and brain-computer interfaces. Determining criminal guilt and estimating the probability of future criminal behaviour are just a few of the legal and societal ramifications.

Cybersecurity [4] has its roots in the early days of computing, where the chief concern was to secure individual systems with the shift in focus as technology advanced and networks emerged towards safeguarding interconnected systems. The exponential growth of the internet in the late 20th century amplified both the opportunities and threats associated with cyberspace with 21st century witnessing an unprecedented surge in cyber threats, ranging from simple viruses to sophisticated cyber espionage campaigns. The rapid digitization of critical infrastructure, financial systems, and personal information intensified the need for robust cybersecurity measures. Key components of cybersecurity include network security, endpoint security, identity and access management (IAM), data security, application security, incident response and recovery, and security awareness and training [5].

The nexus between neuro-ethics and cybersecurity offers an intriguing and challenging terrain in the ever-changing field of cybersecurity, where innovations in technology constantly alter the danger picture. The field of neuro-ethics explores the moral issues raised by neuroscience and the use of information about the brain. The significant areas of interest include:

Biometric authentication [6] is the one where neurology and cybersecurity blends including facial recognition, voice authentication, and fingerprint scanning, relying on distinct physiological and behavioural traits. With the advancement of neuroscience, there is a growing interest in using neurobiological data for increased security, such as brainwave patterns or even brain-based authentication. The prime advantages include enhanced security offering a more reliable and customized type of authentication with lower possibility of unwanted access and convenient user experience which does not require the need to remember passwords or PINs.

Comprehending the neurological systems that underlie human decision-making and behaviour can facilitate the development of advanced social engineering attacks [7]. Cybercriminals may take use of cognitive biases and brain weaknesses to trick people into disclosing private information or acting against their better judgement. Neuro-influenced social engineering can provide very precise and convincing attacks, which might make it difficult for victims to recognise malevolent intent along with leaving a significant psychological effect on them.

Insider threat detection is being investigated with the use of neurotechnology [8], including methods like electroencephalography (EEG) and functional magnetic resonance imaging (fMRI). Organisations monitor brain activity in an effort to spot irregularities that could point to insider threats or criminal inte Neurotechnology may be able to identify stress or malevolent intent in workers before more conventional markers show up signs of malbehaviour. Insider threats are a serious danger to an organization's cybersecurity, but they may be lessened with early identification.
Technologies for cognitive improvement, including brain stimulation or nootropics, are being investigated to improve cybersecurity experts' cognitive capacities. Enhancing concentration, decision-making, and problem-solving abilities is the goal in a field where prompt and precise replies are critical performing better in more efficient threat identification and response with enhanced cognitive resilience [9-10].

1. NEUROSCIENTIFIC TECHNIQUES IN CYBER SECURITY:

2.1 Brain-Computer Interfaces (BCIs): Bridging the mind and machine

Brain-computer interfaces (BCIs) [11] are a rapidly evolving technology that can alter dramatically human interaction with computers to measure brain activity and translate it into commands for a computer or other device, allowing users to control machines and devices using only their thoughts divided into unidirectional and bidirectional categories based on action direction. This intersection of neurobiology and computing has the capability to alter dramatically various aspects of human life, from healthcare and rehabilitation to communication and entertainment, operating through various modalities which includes electroencephalography (EEG), functional magnetic resonance imaging (fMRI), electrocorticography (ECoG), and invasive neural implants that metamorphose external commands into electrical signals transmitted through the nervous system. In functional near-infrared spectroscopy (fNIRS), magnetoencephalography, and electrocorticography, the electroencephalogram (EEG), giving a visual image of the brain activity and track sleeping patterns, diagnose and treat neurological conditions, and investigate cognitive functions offering excellent levels of precision is a commonly used instrument for tracking electrical activity in the brain which quantify various neuronal subtypes in the human brain. Depending on the neural signals recording, it can be bifurcated into invasive and non-invasive BCI [12].
Invasive BCI offers three prime advantages [13]: (1) it can take down activities from every single neuron or modulate the activities of a small population of neurons with much greater spatial and temporal resolution [14]; (2) it has a higher signal-to-noise ratio (SNR) and more resilient to electrical noise interferences or movement artefacts; and (3) its electrodes can be placed in close proximity to or directly in the target cortical areas or subcortical structures. Along with the advantages, it also offers numerous disadvantages [13]. Firstly, the direct insertion of electrodes into brain tissues necessitates an intrusive surgical procedure that raises the possibility of problems. Second, the system requires considerably greater dependability and reduces some degree of flexibility because it is impossible to replace any component or correct hardware issues after it is implanted. Finally, the cost of invasive BCI has to be addressed in order to make it more accessible because of the intricacy of the surgical technique and the post-operation care required.
Non-invasive Brain–Computer Interfaces (BCIs) [13] use techniques including (MEG), (EEG), (fMRI), and (fNIRS) to gather data on brain activity without the need for brain surgery. It takes into consideration the activities through surgically inserted electrodes in close proximity to the targeted neurons in the cortex or deep brain structures. There are benefits such as safety, accessibility, and less invasiveness. On the other hand, its temporal and geographical resolution as well as signal quality could be limited. Noise, artefacts in movement, and the incapacity to distinguish between various parts of the brain can all affect data from non-invasive brain imaging (BCI) as they rely so heavily on measurements from the scalp surface, making it difficult to reliably record deep brain activity. Because everyone's

scalp and skull are different, BCI's utility and reliability might vary as well. Furthermore, significant preprocessing and signal analysis—which can be laborious and computationally demanding—are needed to extract useful information from BCI data.
Brain-computer interfaces (BCIs) rely on electroencephalograms (EEGs) [15] to obtain brain wave data and facilitate brain-to-external device connection, used for a variety of purposes, such as motor imagery (MI), in which people visualise carrying out a certain movement. The ability to comprehend imagined movements and operate external devices has showed promise for EEG-based MI-based BCIs. Wearable EEG devices have further broadened BCI applications, offering more easy and accessible ways to track brain activity.

2.2 Neuroimaging techniques:

The non-invasive surveillance of the structure and activity of the brain is made possible by neuroimaging, an essential technique that clarifies the capabilities that various brain areas play in behavioural and cognitive tasks including language, choice-making, emotion control, insight, attention, and memory [16,17]. When examining brain function, particularly in severe mental diseases like bipolar disorder, neuroimaging is very significant as it evaluates therapy outcomes. Through neuroimaging, scientists may map neural networks, see how the brain functions, and investigate the processes underlying a range of neurological conditions [18]. On deeper understanding the anatomy and function of the brain, it has become much more accurate and detailed with the recent developments in neuroimaging methods helping researchers get an exact picture of the brain's structure, including the sub-millimeter structures of the cortex using high-resolution structural magnetic resonance imaging, facilitating the mapping and identification of unidentified brain areas [19,20].
With an emphasis on human thought, emotion, and behaviour, cognitive biometrics is a novel approach to biometric technology that combines physiological and behavioural traits wherein biosignals pertaining to cognitive and emotional processing are the foundation of it originating from the brain, heart, and autonomic nerve systems [21]. Users may be protected, privacy compliance is ensured, and there is resilience against manipulation using cognitive biometrics [22]. Their non-volitional nature and internal nature shield them from public scrutiny, which reduces their susceptibility to spoofing assaults. Unless the user actively engages in the process, it is unlikely that these biosignals will be detected remotely or in secret using the sensor technologies available today [22, 23].
Users are shielded from presentation assaults by cognitive biometrics, which also provide liveness detection and continuous apps. Because they are not static, biosignals may also be cancelable. Brain biometrics [24] based on event-related potentials enable for the substitution of compromised biometric identifiers with new ones, a capability not accessible in standard biometric modalities like tracks, palmprints, and iris. The benefits of cognitive biometrics have prompted several papers on the subject, highlighting the need for more study and guidance in this area.

3. NEURO-ETHICAL CONSIDERATIONS IN CYBERSPACE:

Neuro-ethics in cybersecurity has emerged as a result of the deep ethical problems raised by the junction of neuroscience and cybersecurity with technologies penetrating the workings of the human mind giving rise to the ethical considerations for use of neuro data. It has emerged as a response to the believe that the frontiers of the skull mark the boundary between the observable and unobservable dimensions of a living person. However, recent advances in neuroscience and neurotechnology has made it possible to unlock the potentials of human brain and throw light on how various brain functions relate to observed behaviour and mental states [25]. Privacy concerns are significant in neurosecurity or cybersecurity, as neurodata captures intimate details of an individual's thoughts and mental states necessitating the defining of boundaries for curation, storage and utilisation of neural data [25, 26]. Standards and regulatory frameworks for neurosecurity or integration of neuroscience in cyber security are crucial,

and neuroethics plays a role in developing the rules guiding the moral use of brain-computer interfaces (BCIs), neural tracking, and cognitive security techniques [27].

The inner workings of human psychology could be altered by neurotechnology, opening the door for external impact on basic human values like agency, mental privacy, and biographical identity. It is crucial to understand that these dangers are neither special nor unique, though, since a large body of research highlighting this fragility makes use of commonplace social manipulation techniques like verbal communication [28]. Modifying the brain and, thus, human agency, identity, and privacy with accuracy and efficacy is what neurotechnology offers. Still, given how difficult it is to control discussions that might purposefully or unintentionally change someone's memory compared to consciously changing memories using BCI, neurotechnologies might be more open to public scrutiny than social manipulation [29, 30]. The slightest alteration in the neural information of brain data can pose significant risks of increased mal-intentions of cyber criminals leading to sophisticated attacks like phishing, vishing, identity theft, ransomware, brainjacking [32] and much more.

Cognitive liberty [34], a concept rooted in autonomy and freedom of thought, is increasingly in talks with relation to emerging technologies that interact with the human mind encompassing the right to autonomy and control over one's cognitive processes, as well as the ethical challenges posed by manipulation and coercion. Autonomy and control pose as the fundamental aspects, emphasizing the right to govern mental processes, thoughts, and decisions without external interference while ethical considerations include informed consent, privacy-preserving technologies, and user-centric design [33]. Manipulation and coercion [34] pose significant ethical challenges about the unintended consequences of influencing or coercing cognitive processes, challenging the essence of individual freedom resulting in the reveal of personal identity as well as information like banking details with ease in the hands of cyber criminals delineating the areas of infringement of individual's rights in autonomous decision making.

While there might be major scientific and therapeutic benefits, the capacity to record and modify brain activity via implantable and non-implantable neural devices also presents difficult ethical questions endangering individual neuro-privacy deciphering unfettered and trading neuro data [31]. Developing legal safeguards specifically addressing the ethical use of neuro-technologies can provide additional protection against manipulation and coercion. Examples include cognitive enhancements in employment, where employees may feel compelled to enhance their cognitive abilities to meet job expectations, and neurotechnological marketing influence, where advertisers may manipulate consumer preferences or decision-making processes [25,33,35]. The development of neuro data guidelines [26] is the primary concern to safeguard individuals from the clutches of cybercriminals who are prone to trick individuals into revealing confidential data and misusing it with more vigor and ease and performing activities like brain hacking. The above mentioned ethical issues pose a considerable need for the development of framework with experts in the field of neuroscience, ethics, neurotechnology and cybersecurity.

4. CONCLUSION

Neurotechnology applications are growing rapidly both on the inside as well as on the outside of the clinical and research setting in terms of volume and variety making the availability of more affordable, scalable, and user-friendly neuro applications. In terms of clinical benefit, prevention, self-quantification, bias reduction, personalized technology use, marketing analysis, military dominance, national security, and even judicial accuracy, this technological trend may be extremely advantageous for society as a whole. However, its implications for ethics and the law are yet to be taken care of. A proposal that the normative landscape needs to be established swiftly to prevent misuse or unanticipated negative repercussions, given the disruptive revolution that neurotechnology is bringing about in the digital environment. The emergence of neuroscience in the domain of cybersecurity poses the question of ethical considerations of the use of neuro data which has been highlighted in this paper. A need for

proper guidelines and framework at global scale to prevent misuse of data and impart proper ethical standards is the need of the hour safeguarding individual's right to privacy.

REFERENCES

[1] J. Das et al., "Neuroscience is ready for neuroethics engagement," Front. Commun., vol. 7, p. 909964, 2022.

[2] M. Ienca et al., "Towards a governance framework for brain data," Neuroethics, vol. 15, no. 2, p. 20, 2022.

[3] Kritika, "Cyber Security and its cognitive ramifications on e-governance," IJIRMF, vol. 9, no. 5, 2023.

[4] Kritika, "Demystifying Cyber Crimes," in Perspectives on Ethical Hacking and Penetration Testing, K. Kaushik and A. Bhardwaj, Eds. IGI Global, 2023, pp. 63–94. [Online]. Available: https://doi.org/10.4018/978-1-6684-8218-6.ch003

[5] J. Jain and P. R. Pal, "A recent study over cyber security and its elements," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3, pp. 791–793, 2017.

[6] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," J. Imaging, vol. 9, no. 9, p. 168, 2023.

[7] F. Babiloni and P. Cherubino, "Consumer Neuroscience: A Neural Engineering Approach," in Handbook of Neuroengineering, Singapore: Springer Nature Singapore, 2023, pp. 2861–2889.

[8] J. A. Olson et al., "Emulating future neurotechnology using magic," Conscious. Cogn., vol. 107, p. 103450, 2023.

[9] Y. Eski, A Criminology of the Human Species: Setting an Unsettling Tone. Springer Nature, 2023.

[10] N. Liv and D. Greenbaum, "Cyberneurosecurity," in Policy, Identity, and Neurotechnology: The Neuroethics of Brain-Computer Interfaces, Cham: Springer International Publishing, 2023, pp. 233–251.

[11] J. Peksa and D. Mamchur, "State-of-the-Art on Brain-Computer Interface Technology," Sensors, vol. 23, no. 13, p. 6001, 2023.

[12] M. A. Lebedev and M. A. Nicolelis, "Brain-Machine Interfaces: From Basic Science to Neuroprostheses and Neurorehabilitation," Physiol. Rev., vol. 97, pp. 767–837, 2017.

[13] Z. Zhao et al., "Modulating Brain Activity with Invasive Brain–Computer Interface: A Narrative Review," Brain Sci., vol. 13, no. 1, p. 134, 2023, doi: 10.3390/brainsci13010134.

[14] S. Saha et al., "Progress in Brain Computer Interface: Challenges and Opportunities," Front. Syst. Neurosci., vol. 15, p. 578875, 2021.

[15] A. Saibene et al., "EEG-Based BCIs on Motor Imagery Paradigm Using Wearable Technologies: A Systematic Review," Sensors, vol. 23, no. 5, p. 2798, 2023, doi: 10.3390/s23052798.

[16] M. C. Litwińczuk, N. Trujillo-Barreto, N. Muhlert, L. Cloutman, and A. Woollams, "Relating cognition to both brain structure and function: A systematic review of methods," Brain Connect., vol. 13, no. 3, pp. 120–132, 2023.

[17] T. Morita, M. Asada, and E. Naito, "Contribution of neuroimaging studies to understanding development of human cognitive brain functions," Front. Hum. Neurosci., vol. 10, p. 464, 2016.

[18] C. Yen, C. L. Lin, and M. C. Chiang, "Exploring the frontiers of neuroimaging: a review of recent advances in understanding brain functioning and disorders," Life, vol. 13, no. 7, p. 1472, 2023.

[19] C. Zeng et al., "Advanced high resolution three-dimensional imaging to visualize the cerebral neurovascular network in stroke," Int. J. Biol. Sci., vol. 18, no. 2, pp. 552–562, 2022.

[20] E. B. Vanstrum et al., "Development of an ultrafast brain MR neuronavigation protocol for ventricular shunt placement," J. Neurosurg., vol. 138, no. 2, pp. 367–373, 2022.

[21] M. Wang, X. Yin, Y. Zhu, and J. Hu, "Representation learning and pattern recognition in cognitive biometrics: a survey," Sensors, vol. 22, no. 14, p. 5111, 2022.

[22] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 7, pp. 1618–1629, 2016.

[23] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: an evaluation methodology and lessons learned," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015.

[24] Q. Gui, M. V. Ruiz-Blondet, S. Laszlo, and Z. Jin, "A survey on brain biometrics," ACM Comput. Surv., vol. 51, no. 6, pp. 1–38, 2019.

[25] M. Ienca and R. Andorno, "Towards new human rights in the age of neuroscience and neurotechnology," Life Sci. Soc. Policy, vol. 13, no. 1, p. 1, 2017.

[26] H. T. Greely et al., "Neuroethics guiding principles for the NIH BRAIN initiative," J. Neurosci., vol. 38, no. 50, p. 10586, 2018.

[27] S. Burwell, M. Sample, and E. Racine, "Ethical aspects of brain computer interfaces: a scoping review," BMC Med. Ethics, vol. 18, no. 1, pp. 1–11, 2017.

[28] S. Rainey et al., "Data and Consent Issues with Neural Recording Devices," in Clinical Neurotechnology meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications, 2021, pp. 141–154.

[29] S. Goering et al., "Recommendations for responsible development and application of neurotechnologies," Neuroethics, vol. 14, no. 3, pp. 365–386, 2021.

[30] E. Hildt, "What will this do to me and my brain? Ethical issues in brain-to-brain interfacing," Front. Syst. Neurosci., vol. 9, p. 17, 2015.

[31] R. Yuste, "Advocating for neurodata privacy and neurotechnology regulation," Nat. Protoc., vol. 18, no. 10, pp. 2869–2875, 2023.

[32] L. Pycroft et al., "Brainjacking: implant security issues in invasive neuromodulation," World Neurosurg., vol. 92, pp. 454–462, 2016.

[33] P. Sommaggio and M. Mazzocca, "Cognitive Liberty and Human Rights," in Neuroscience and Law: Complicated Crossings and New Perspectives, 2020, pp. 95–111.

[34] B. C. M. M. is Mine, "Cognitive Liberty as a Legal Concept," in Cognitive Enhancement. An Interdisciplinary Perspective, E. Hildt and A. G. Franke, Eds. Dordrecht: Springer, 2013, pp. 233–264.

[35] T. Istace, "Neurorights: The Debate About New Legal Safeguards to Protect the Mind," Issues L. Med., vol. 37, p. 95, 2022.

[36] R. Rupp et al., "Brain–computer interfaces and assistive technology," in Brain-Computer-Interfaces in their ethical, social and cultural contexts, 2014, pp. 7–38.

[37] N. Rose, "The human brain project: social and ethical challenges," Neuron, vol. 82, no. 6, pp. 1212–1215, 2014.