



SECURITY APPROACHES IN NEROSCIENCE

P.Muthu Subramanian¹, A.Rajeswari²

^{1,2} Department of Electronics and Communication Engineering
^{1,2} Coimbatore Institute of Technology, Coimbatore

¹pmuthusubramanian1@gmail.com, ²rajeswari.ece.cit@gmail.com

ABSTRACT:

In order to enhance Cybersecurity performance by people, we are striving to comprehend the neurological elements of cyber security ability. Attackers who target computer security are referred to as "hackers" in this article. In order to explore pattern classification, thinking, and choice function that facilitate the identification and manipulation of security flaws, our initial objective is to develop behavioural accuracy and response time metrics. The development of theories addressing issues relating to the identification, measurement, and training of cyber security expertise will be facilitated by an understanding of the intellectual processes involved. In addition to behavioural tests, our objective is to conduct a structural neuroimaging research of the neurological process systems which can identify individuals with varying levels of knowledge about security approaches. Our next objective is to empirically evaluate how attackers' thought processes—which psychologists refer to as biases and heuristics affect how susceptible they are to security methods. With the help of deceptive or fraudulent content, honeypots are a tried-and-true method for diverting attackers' attention away from legitimately critical data and their limited time and skills are being wasted. The ultimate objective is strengthening the present system security, we analyse hackers' minds using the vast experiments and studies we have conducted to look inside the minds of skilled grandmasters.

Keywords: Cyber security, neuroscience

DOI Number:10.14704/nq.2022.20.8.NQ44390

NeuroQuantology 2022; 20(8): 3614-3619

I Introduction

Understanding competence in computer fields related to cyber security is something we must undertake immediately and with increasing urgency. There are still ongoing cyber threats to information systems, infra structure, and software solutions increase as the world becomes more dependent on digital services for transactions, information preservation, and social relationships. Cybersecurity threats can take off from any location worldwide and can intended to commercial or governmental

eISSN1303-5150

goals, allowing for significant intrusions of privacy and interference with routines. One of the most concerning revelations is that sectors producing packaging materials, wastewater treatment facilities, and the electrical grid are all vulnerable to cyberattacks [1]. It will be required to have a greater knowledge of the human aspect involved in cyber conflict, particularly on the offensive side, in order to foresee, analyse, and fight against such cyber security risks [2]. In addition to researching how people behave in relation to cyberattacks, it will become

www.neuroquantology.com



identification is becoming more crucial personal characteristics that are cyber-predictive abilities it is beneficial for the defence. Significant yet unanswered problems about human talent and cyber knowledge are still unresolved. These include fundamental queries like what types of people are proficient in cyber capabilities and how the necessary talents can be recognized and assessed. In the proposed approach, we put the most emphasis on answering these concerns from the standpoint of cognitive expertise [3]. Experts are characterised outstanding abilities in a given field, and their abilities can be evaluated through laboratory tests in comparison to those of beginners or newcomers [4]. The cognitive viewpoint has a long history of researching expertise, but most of this work has concentrated on sports [5], activities [6], or a small number of professional fields, such health [7] and medicine [8]. By way of evaluation proficiency on a range of confront issues that necessitate the use of certain abilities in order to solve them, we concentrate on defining and establishing standards for professional performance in cyber competence. We want to measure and evaluate these abilities in accordance with their level of difficulty in order to produce a series of competence ratings related to solving problems on the internet or hacking. An essential first step in finding talent in this industry is to experiment with assessing and measuring technical expertise relevant to cyber security. The need for skilled workers on the human operations end will increase as societies develop to move greater network and data management in cyberspace. This might be particularly relevant for cyber security, where constant threat mitigation and monitoring will be required as threats alter and arise. In order to effectively defend against cyber security attacks, it is essential to comprehend the abilities, motives, and talents of the attacker. Cyber experts are not likely to be effective general problem solvers. Instead, we must discuss what precise skills in what speciality fields are crucial to cyber expertise [3], as is

the case in the majority of other fields of human knowledge. These speciality areas' identities and potential connections with one another are unknown. Thus, starting to make progress in this area of study is a crucial beginning objective of the current project. Training in cyber security is becoming more and more necessary. In addition to identifying those with a proclivity for hacking or cyber security, it's critical to put these people through training. A variety of computer science courses and lab experiences are available now that are helpful for educating people about software and hardware requirements for cyber security. Training that focuses on comprehending the human element in this field is currently lacking. This involves knowledge of the motivations, propensities, and skills of attackers, how to spot them, and the best ways to protect against different types of assailants.

II Cyber Security in Neuroscience

Understanding expertise with cognitive neuroscience: To further investigate cyber expertise, we need to use neuroimaging techniques in addition to merely behavioural studies. The study of cognitive psychology has been changed by modern such as functional mri, are used in neuroimaging, which provide more information about the neurological systems that underlie memory, thinking, and decision-making. In previous research we used blood oxygen level dependent (BOLD) signalling to measure task-based brain activity in order to examine questions concerning the nature of expertise. The key techniques that enable new conclusions on skill using this strategy are the cautious creation activities that represent an individual kind of skill and comparing circumstances that are comparable in numerous ways other than significantly avoid reflecting an individual's skills. The benefit of neurological approaches what can support traditional behavioural measures by subtly disclosing details about the parallels or discrepancies between experimental environments. When paired with accuracy and reaction times, this is especially helpful



for solving issues or reacting to stimuli. Our earlier research on chess mastery provides an illustration of the value of integrating behavioural and fMRI studies. In these experiments, we compared how people perceive chess-related configurations visually to how they perceive images of people's faces, a field in which almost everyone has a high level of proficiency. We must be able to quickly and easily recognise faces in order to function socially. Our ability to distinguish faces helps us quickly identify and decipher the intents of strangers we have just met. Similar to this, a skilled chess player may quickly assess the state of a game by watching the eventual winner, the margin of victory, and the locations of direct targets and chances. These skills have a striking resemblance to the rate and precision of recognition seen in individual features recognition. In an interference paradigm, we conducted an experiment to see if chess professionals' face and chess perception were similar. According to the findings, chess and facial stimuli showed comparable degrees of interference, a sign of experience [9]. At first glance, it would seem that facial perception and chess expert perception are very similar. In a subsequent experiment, We compared the visual cortex's activation in response to stimuli linked to faces and chess using MRI. As evidence that the two areas of knowledge share overlapping mechanisms, we had predicted that there would be overlap in brain activity. Contrary to what we expected, professionals showed very little overlap in their judgement of faces and chess [10]. The idea that behavioural level assessments of knowledge can only give a partial picture of how expertise develops and is organised is highlighted by this pair of findings. This lesson might be even more crucial in more intricate fields. We must design and perform a series of fMRI studies with experimental settings that connect processes important to cybersecurity knowledge and unfavourable control circumstances. This will make it possible for us to create new expertise markers that are pertinent to kinds of knowledge in cyber

security. These indicators might next be connected to individuals' results on the bias-susceptibility test as well as to the results from the tests we will create to gauge different sorts of cyber competence. Better defence will result from understanding offence: Measuring the abilities necessary to carry out attacks is a crucial component of comprehending cyber expertise. The ability to better inform instructing opponents on where to look for attacks as well as how to identify them, and how to mitigate against them would result from knowing the skills of attack-side hackers. The vulnerability of attackers to detection and delay is an important topic of research (Examine how cognitive shortcuts and flaws affect cyber security attack scenarios where avoiding hazards is necessary). Key biases that people have operating within them have been uncovered by research on judgement and decision-making. As people gain skill, certain of these biases have a tendency to become harder to overcome and more embedded [11]. These biases exist across disciplines and have defied efforts to eradicate them if cognitive biases were known; the organization would be able to utilize this data to enhance protection solutions. mechanisms could be better understood. The following are a few of the strong cognitive biases that have been demonstrated to exist in experts:

- Performing an ineffective series of acts that have previously been successful irrationally is known as "setting effects" [12]
- Confirmation bias is the propensity to seek out data that supports a preferred belief. Wason(1960 & 1968)
- "Sunken cost reasoning" which refers to the propensity to remain with a particular method because it has received a lot of earlier effort[13]
- "representativeness" which refers to a situation's appearance of similarity to structurally dissimilar circumstances from the past [14].
- "availability" which refers to how simple it is to think back on previous examples of a particular activity being successful [15].



In situations involving cyber defense-side security, where a hacker needs to speculatively deduce, make attempts to learn more. These biases are likely to occur throughout fields and provide significant challenges whenever an encounter given confusing information, before even being able to attack a machine. Biases are connected to heuristics, which are realistic shortcuts or presumptions that frequently function well in a variety of settings. High levels of efficiency result from using heuristics since they allow for quick decisions that are usually accurate. Heuristics do have a drawback, too, in that they can occasionally be misused in unique circumstances. Heuristics can be misused to draw erroneous conclusions and errors in logic. Humans frequently use heuristics, especially when they have a high level of informational familiarity and proficiency, including high levels of competence. Heuristics can be applied excessively or incorrectly in situations when a higher level of skill places an attacker in a vulnerable position. If defenders knew the types of biases typically employed by various categories of attackers, they could take advantage of these flaws.

The second specific purpose, "Attracting Attackers Using Honeypots," focuses on the connection between heuristics and biases and expertise. Defense-side cyber security experts may be able to create honeypots, baits, and pitfalls to lure and deter invaders if they can recognise how unique biases operate in various kinds of attack specialisation. Using fake content that is superficially appealing to an attacker, honeypots and honeynets are often used techniques to catch attackers [16]. By ostensibly imitating a real system and using actual sensitive information, they draw an attacker. Since most honeypots lack authentic material and offer no justifiable purpose for a person to use their services, any behaviour inside of one might be viewed as harmful. It is in the defender's best interest to keep the hacker there once they have been drawn to the honeypot. The more time and resources

an attacker wastes dealing with the honeypot, the more they divert their attention away from real services, real data, and real processes. Additionally, defenders can observe an attacker's operations and tactics to learn more about their objectives and strategy by using a honeypot [17]. By making use of awareness of heuristic utilisation and cognitive bias, the objective of keeping an attacker in a honeypot can be made easier. If the honeypot proves to be uninspiring or, perhaps worse, a trap, the attacker is likely to leave it alone despite its first enticing appearance. As a result, creating engaging honeypots effectively requires them to do so. By using information of neurological prejudices in humans, defenders can force attackers to spend more of their resources while they are caught in honeypots for longer periods of time. By examining the influence of Set effects, confirmation bias, representativeness, and availability are all examples of biases that are likely to slow down operations and exacerbate the issues honeypots place on attackers, we want to explore how this may be accomplished.

III SURVEY

Our strategy is based on the preliminary research we have done on the behaviour of expert chess players. We will modify these techniques to investigate cyber security and how individuals and organisations of hackers think and act. These studies are listed below.

The tools of cognitive psychology are an effective instrument for the investigation of expertise. Researchers have linked numerous distinct features of face processing to either face-specific systems or significant experience telling apart faces. Investigation is on the brain underpinnings of cognitive processes using fMRI techniques. We looked into whether the processing of faces and chess moves in the brains of chess masters to see if there were any parallels. Chess and faces should elicit equivalent regional activations of perceptually relevant visual cortex if the neural responses to the two stimuli are similar. This theory would seem to



be supported by the results of Preliminary Study 1. However, if skill is organised differently inside the brain and different types of expertise operate differently, we might not notice a great deal of overlap between the cerebral activity linked to understanding faces and chess.

IV PROPOSED APPROACH

In order to specifically support the system approach, which aims to characterise and evaluate We seek to create behavioural tasks that adequately represent important facets of offensive cyber security in order to understand cognitive factors of real concern and outcome in cyber security expertise. The evolution and use of fMRI exercises that reflect insight on the apprehensive foundations of the numerous sections of cyber competence will assist the proposed approach. We will then construct resolving issues that include honeypots that has to be discovered and ignored in order to test the impact of assumptions and behavioral shortcuts in cyber security assault under circumstances demanding avoiding pitfalls. By designing the test-bed honeypots to capitalise on well-known cognitive biases, we can determine which concerns are most likely to deter attackers by gauging how well people do on them. A critical first step in solving issues is assessing ground details to assess its likelihood of further investigation. In order to better understand how cyber professionals evaluate stimuli for significance before paying them greater attention in actual cyber settings, neuroimaging will be used. We will concentrate on ten categories, including URL redirection, buffer breach, OS code injection, and Cross site scripting, incomplete identification, incomplete authorisation, wrong permission, a bug in the integer, and use of inappropriate rights, and the execution of risky operations. We anticipate that professionals will be able to identify programming flaws and eliminate pointless code. The activation of BOLD in these processes will show whether spotting exploitable flaws is equivalent to spotting coding errors alone, and it will also show

whether neural activation varies depending on expertise level inside areas of interest or error checking parts of the brain. An essential component of fMRI research is the development of very comparable control conditions to the situations of interest. Participants will see lines of typical code consecutively and for two seconds at a time in this experiment. There will occasionally be an intriguing weakness in a code sequence. These trials will be fascinating. Code with a syntax error will be present in the control stimuli. It is critical to note that while these stimuli will appear to superficially match Behavioural vulnerability triggers and response identification call for similar behaviour method, they will not be similarly pertinent to cyber assault. In a third example, the code lacks interest opaque, and it simply needs to be pressed once to reveal a pre-programmed sentence that is embedded in some screens.

V CONCLUSION

As was discussed in this essay, we must investigate hackers' thoughts in order to build better systems. We will specially integrate behavioural and neurological technologies, comprising fMRI techniques, to investigate the thoughts behind hackers. The preliminary research we've done on studying the chess players' thinking has shown positive results. I think that applying our techniques can enhance internet safety. Additionally, we think in order to stop cyberterrorism, must constantly outwit hackers. Consequently, creating safe systems without initially comprehending the various categories of hackers won't be the ideal practise. Our strategy incorporates the two, examining hackers' minds, securing system upgrades, and using the insights acquired from behavioural and research into the brain to enhance systems. The intended investigations will result in new behavioural and cognitive metrics that will be useful in several important fields of computer security knowledge. These studies will specifically: offer new methods for identifying subtypes of cyber security specialists; offer fresh insights



into the aptitudes, drives, and propensities of offensive-side hackers; offer assessments Considering the varieties of cognitive distortions most common in attacker subtypes offer proof among those deception methods that could be most advantageous for the creation of honeypots; and offer infrared imaging. Additionally, all data obtained for this project will have a wide range of applications for educating cyber professionals and detecting offensive trends and talents that may be used to improve defence strategies.

REFERENCES

[1] Cyberware 2011 Westport, CT: Praeger.
[2] Pfleeger, SL & Caputo, D.D. : Leveraging behavioral science to mitigate cyber security risk.
[3] Ericsson K . A. ;, Expertise. Tyler J. Towne. Article first published online: 22 APR 2010 . DOI: 10.1002/wcs.47. Copyright © 2010 John Wiley & Sons, Ltd.
[4] Chi, M.T.H. (2006). Methods to assess the representations of experts' and novices' Knowledge . In K.A. Ericsson, N. Charness, P. Feltovich, & R. Hoffman (Eds.), Cambridge Handbook of Expertise and Expert Performance. (Pp. 167-184), Cambridge University Press.
[5] Gobet, F., & Charness, N. (2006). Chess and games. Cambridge handbook on expertise and expert performance (pp. 523-538). Cambridge, MA: Cambridge University Press.
[6] Duffy, L. J., Baluch, B., & Ericsson, K. A. (2004). Dart performance as a function of facets of practice amongst professional and amateur men and women players. International Journal of Sport Psychology, 35, 232-245.
[7] Ericsson, K. A. (2007). An expert-performance perspective on medical expertise: Study superior clinical performance rather than experienced clinicians! Medical Education, 41, 1124-30.
[8] Harley, E. M., Pope, W. B., Villablanca, P., et al. (2009). Engagement of fusiform cortex and disengagement of lateral occipital cortex in the acquisition of radiological expertise. Cerebral Cortex, 19: 2746–54.

[9] Boggan, A. L., Bartlett, J. C., & Krawczyk, D. C. (2012). Chess Masters show a hallmark of face processing for chess. Journal of Experimental Psychology: General, 141, 37-42.
[10] Krawczyk, D. C., McClelland, M. M., & Donovan C. (2011). A hierarchy for relational reasoning in the human prefrontal cortex. Cortex, 47, 588-597.
[11] Bilaliü M, McLeod P, Gobet F (2010) The mechanism of the Einstellung (Set) effect: a pervasive source of cognitive bias. Curr Direct Psychol Sci 19:111–115.
[12] Luchins, A. S. (1942). Mechanization in problem solving. Psychological Monographs, 54, No. 248.
[13] Arkes, Hal; Blumer, Catherine (1985). "The Psychology of Sunk Cost". Organizational Behavior and Human Decision Process 35: 124–140.
[14] Tversky, A. & Kahneman, D. (1974). Judgments and Uncertainty: Heuristics and Biases. Science, New Series, 185 (4157), 1124-1131.
[15] Tversky, A. & Kahneman, D. (1973). Availability: A Heuristic for Judging Frequency and Probability. Cognitive Psychology, 5 (2), 677-695.
[16] Cohen F. (2011) Use of Deception Techniques: Honeypots and Decoys University of New Haven 182. The Handbook of Information Security, Volume III Threats, Vulnerabilities, Prevention, Detection and Management.
[17] Cheswick, B. "An evening with Berferd in which a Cracker is Lured, Endured, and Studied", <http://www.tracking-hackers.com/papers/berferd.pdf> , 1991.

