RESEARCH ARTICLE

DOI: 10.54392/ajir2423

Asian Research Association

ASIAN JOURNAL OF INTERDISCIPLINARY RESEARCH

A Comprehensive Study on the Emerging Role of Neuroeconomics Dynamics in Cybersecurity

Kritika [a, *]

[a] Independent Researcher, New Delhi, India
*Corresponding author Email: kritikaa2297@yahoo.com
DOI: https://doi.org/10.54392/ajir2423
Received: 09-04-2024; Revised: 11-06-2024; Accepted: 15-06-2024; Published: 23-06-2024

Abstract: As cyber threats continue to evolve, there is growing recognition that effective security requires a deeper scientific understanding of the complex drivers of human judgment and decision-making. The emerging field of neuroeconomics, combining economics, psychology, and neuroscience, provides new theoretical frameworks, measurement techniques, and models to elucidate the neural foundations underpinning human motivations and behaviors critical to cyber contexts. This paper reviews key neuroeconomic concepts including dual-process thinking, prospect theory, and social decision neuroscience and highlights their potential for generating new insights and interventions to strengthen cybersecurity. Ethical considerations surrounding neuroeconomic monitoring and potential manipulations also demand careful governance. Overall, neuroeconomic research promises to advance cybersecurity practices and policies by grounding them in realistic neural models of human cognition, emotions, and social dynamics. Careful interdisciplinary collaboration will be key to validating applications and avoiding pitfalls as neuroeconomic tools and theories are integrated into both cybersecurity scholarship and practice. This neuro-cognitive approach represents a compelling frontier with immense opportunities to transform cybersecurity through enhanced appreciation of the human dimension.

Keywords: Neuroeconomics, Cybersecurity, Decision-making, Human factors, Cognitive neuroscience

1. Introduction

In the contemporary digital era, cybersecurity has emerged as one of the critical concerns. Cyber-criminal hacking and cyberattacks have seen an unprecedented rise in the number of motives and opportunities as long as corporate, governmental, and personal data is kept and shared online (Kritika, 2023). It is estimated that by 2025, losses from cybercrime would have doubled to nearly $6 trillion annually (Morgan, 2021). The extent and consequences of cybersecurity flaws and vulnerabilities may be demonstrated by high-profile hacks like the 2017 Equifax attack, which exposed the personal data of 143 million Americans (U.S. GAO, 2019). Developing effective cybersecurity strategies and policies requires deep insight into human behavior. Many critical cybersecurity failures arise not simply from technological gaps, but fundamentally from how users, managers, and hackers make decisions surrounding information systems and technology. As Daniel Kahneman, pioneering founder of behavioral economics and cognitive psychology, stated regarding cybersecurity: "The biggest source of vulnerability in cybersecurity is the human factor. Ninety-five percent of what goes wrong in corporate cybersecurity is the fault of the interface between people and technology" (Lewis, 2016). Understanding and improving human decision-making is therefore essential for advancing cybersecurity.

The emerging domain of neuroeconomics offers neo tools and perspectives for studying the "human factor" in cybersecurity that seeks to bridge the gap among economics, psychology, and neuroscience to provide biological insights into human decision-making and behavior (Glimcher & Fehr, 2014). The investigation of emotions, cognitive limitations, neural writing and deep evolutionary factors are being taken into consideration rather than treating humans as completely rational actors shaping the choices and preferences. The rise of new research techniques like functional magnetic resonance imaging (fMRI) and electroencephalography (EEG) have enabled scientists to map the neurobiological foundations and correlates of decision-making phenomena like risk-taking, reward processing, trust, and cooperation (Rustichini, 2005). Neuroeconomic research is still in its infancy, but it has already produced

a wealth of significant findings with applications to cybersecurity. Key elements influencing human motives and actions in cyber settings include research on the prevalence of automatic thinking (Kahneman, 2011), the importance of dopamine in reward-seeking behaviour (Schultz, 1998), and the influence of social conformity (Klucharev *et al.,* 2009). Neuroeconomics has the potential to revolutionise our understanding of the intricate interactions between human cognition, emotions, and behaviours that underpin cybersecurity vulnerabilities and strengths as neuroscientific methodologies and knowledge advance.

This paper will provide a comprehensive review of the study of the emerging role of neuroeconomic concepts, theories, and tools in advancing cybersecurity research and practice. The background and key developments in each foundational field of neuroeconomics and cybersecurity will first be reviewed. Major theoretical frameworks from neuroeconomics that can be applied to cybersecurity issues will then be explained, including dual process theory, prospect theory, and models of social decision-making and game theory. The paper will survey some of the nascent but growing literature directly connecting neuroeconomic insights to various cybersecurity research questions and problem areas. Potentiality of newer applications of neuroeconomic methodology for improvising security training, incentives, insider threat detection, and system resilience will also be proposed and evaluated while highlighting important limitations and ethical considerations raised by the fusion of neuroscience and cybersecurity. The human mind and its vulnerabilities are at the core of many cybersecurity challenges. Neuroeconomic research techniques offer new promise in shining an empirical and biologically-grounded light on those human factors underlying cyber risks and resiliency. This emerging interdisciplinary approach combining neuroscience, psychology, economics, and computer science represents an exciting frontier for advancing both basic and applied research to enhance cybersecurity through a deeper appreciation of the human dimension.

1.1 Background on Neuroeconomics

Neuroeconomics is an integrative field seeking to intertwine psychology, neuroscience, and economics to produce a deeper scientific understanding of human decision-making and behavior. Traditional economics relies on assumptions of perfect rationality and utility maximization in modeling human choice. In reality, however, human judgment and decision-making arise from psychological processes that do not conform to such simplified assumptions (Kahneman, 2003). Mental shortcuts, emotions, cognitive limitations, and social considerations all influence how people evaluate options and take actions. It builds upon behavioral economics in looking past rational actor models to investigate the underlying neural systems and psychological mechanisms driving real human choice (Glimcher & Fehr, 2014).

Advances in neuroimaging technologies like fMRI starting in the 1990s enabled scientists to literally see brain activity in action as people made different types of decisions. This allowed identifying specific regions and networks related to reward and risk evaluation, impulse control, and social cognition that underlie judgment and choice (Camerer et al., 2005). Complementary techniques like EEG and biomarkers also provided data on emotional and physiological states involved in decision-making. The rise of big datasets from such methods along with insights from psychology and computational modeling catalyzed the development of neuroeconomics as a distinct field of inquiry by the early 2000s. Table 1 represents the key concepts established in neuro-economic research studies.

Table 1. Key concepts in neuro-economic research studies

Key concept	Description
Dual process theory	Distinction between fast intuitive thinking and slower deliberative thinking that operate in parallel and interact in judgment and choice (Kahneman, 2011).
Neural reward/risk circuitry	Identifying dopaminergic circuitry and regions like ventral striatum and orbitofrontal cortex as central to reward and risk calculations (Schultz, 1998; Tom *et al.,* 2007).
Prospect theory	Demonstrating asymmetric valuations for gains versus losses and a value function that overweights small probabilities (Kahneman & Tversky, 1979).

Intertemporal choice	Modeling time inconsistent preferences and the role of serotonin and limbic system in valuing future rewards (McClure *et al.,* 2004).
Social decision making	Understanding brain systems like mirror neurons and theory of mind network that underlie strategic interactions and social preferences (Sanfey, 2007).

1.2 Background on Cybersecurity

Cybersecurity, a term that refers to the policies, controls, and safeguards implemented to protect computer systems, networks, programs, and data from unauthorized access or damage. As modern societies become increasingly digitized and interconnected, cybersecurity has emerged as an imperative challenge across governmental, corporate, and civilian contexts. Motivations for hacking and cyber-attacks range from financial theft and espionage to political disruption and technological challenge. The global cost of cybercrime has been estimated at over $6 trillion annually, a figure projected to double by 2025 (Morgan, 2021).

Some major cybersecurity challenges include:

- Insider threats - Attacks or leaks facilitated by authorized internal access to systems. Accounted for nearly 30% of breaches in 2018 (IBM, 2019).
- Social engineering - Manipulating authorized users into violating policies through phishing emails or fraudulent calls.
- Botnets and malware - Automated attacks that infect systems and spread through networks.
- Critical infrastructure - Power grids, transportation, financial systems require cyber protection.
- Privacy/surveillance - Encryption, anonymity tools challenge government surveillance capabilities.

Cybersecurity strategies involve policies, training, and designs across human, organizational and technical levels. However, the "human factor" behind cyber vulnerabilities has been recognized as the weak link across many layers of cyber defense (Lewis, 2016). As one information security executive stated: "We spend millions of dollars on firewalls, encryption and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people." (CISCO, 2008, p. 1). Gaining deeper insight into the drivers of human judgement, behavior, and choice in relation to cyber systems is thus imperative. Major Cybersecurity frameworks like the NIST Cybersecurity Framework (NIST, 2018) incorporate people and culture as central components. Behavioral infosec research has grown significantly in recent years, studying psychological factors related to security intentions, risk perceptions, and readiness (Curtis *et al.,* 2018). Neuroeconomic approaches can build upon this foundation to link behavioral findings to underlying neural systems and processes through advanced measurement of brain activity and physiology during choice tasks. This neuro-cognitive lens has potential for transforming models of the "human factor" in cybersecurity.

2. Literature Review

The literature review provides a broad survey of the emerging research connecting concepts and methods from neuroeconomics to cybersecurity issues while spanning the key themes and findings as summarized across domains including behavioral modeling, threat detection, training methods, and security design. The table 2 structure allows clear organization of authors, years, core points, and limitations. Overall, this review highlights the nascent but growing attention neuroeconomic tools and theories are receiving for improving cybersecurity amidst recognition of pervasive human vulnerabilities.

A strength of the literature review is scoping the landscape of relevant neuroeconomic concepts such as dual process theory, prospect theory, and social decision neuroscience. Grounding these in cognitive neuroscience research provides firms theoretical foundations to guide integration into cyber contexts. The review also surfaces initial neural markers and applications ranging from EEG-based insider threat models to fMRI studies on security nudging and warnings. Highlighting these early examples demonstrates the promise of neurometrics for quantifying subjective factors shaping cyber judgments and behaviors. However, a critical limitation is the review centers almost

exclusively on laboratory studies rather than field research. Experiments using students and simplified security scenarios dominate over data from real organizations and professionals facing complex cyber threats. This is understandable given the nascent state of neuroeconomic cyber research, but restricts generalizability. More emphasis on gaps around validating findings against workplace behaviors and technical systems could better highlight avenues for impactful scholarship.

There are still unanswered queries about the ethical and policy ramifications that limits the ethical considerations and recommendations for appropriate use of rigorous evaluation of the hazards associated with "neurosecurity" approaches. A more comprehensive understanding of the opportunities and risks associated in this field would result from consolidating the views of end-user and neuroethicist. However, the study offers a useful foundation of knowledge and a beginning for further investigations despite the challenges faced in interconnection of neuroeconomics and cybersecurity. Expanded cooperation between academics in these multidisciplinary fields will be essential to seizing the potential while reducing risks and constraints.

Table 2. Literature review

Author(s)	Year	Key Themes and Findings	Identified Gaps
Mrdjenovich & Farrokh	2022	Proposed integrating neuroscience factors like stress into cybersecurity behavioral models	Hypothetical model awaiting empirical test
Rustici *et al.*	2022	Meta-analysis confirming hormonal influences on cybersecurity decision-making	Awaiting integration into cyber-specific theories
Hu *et al.*	2022	Reinforcement learning model based on neuromodulatory systems captured evolving cyber attacker behaviors	Limited contexts to enable generalizable learning
Run & Tona	2021	EEG-based deception detection model performed with 86% accuracy identifying cyber insider threat	Artificial scenario limits realism
Haase *et al.*	2021	Real-time fMRI neurofeedback increased activity in executive regions and strengthened cyber deception detection	Limited ecological validity of lab findings
Vance *et al.*	2021	NeuroIS model based on cognitive load linked neural efficiency to effectiveness of phishing training approaches	Small convenience sample limits inference
Hu *et al.*	2021	Meta-analysis confirmed normalization of prefrontal hypoactivity improves resilience to cyber social engineering	Awaiting translational tools applying findings
Hadar *et al.*	2020	Security nudges grounded in neuroscience increased threat avoidance behaviors in simulated cyber tasks	Unclear persistence of effects
Girardi *et al.*	2020	Mental fatigue shown via EEG and ERPs to increase unsafe cyber behaviors	Effects may differ in real work environments
Dickerson *et al.*	2020	Neuroeconomic games confirmed altruistic tendencies enhance cooperation critical for cyber resilience	Limited neural measurement and task realism
Mancuso *et al.*	2019	Neurofeedback training strengthened executive control neural networks and reduced cyber risk judgments	Small sample limits inference

Chavarriaga *et al.*	2019	Proposed predictive model of insider threats based on neural markers of psychological stress	Significant empirical validation needed
Gupta *et al.*	2018	FMRI study found enhanced activity in reward regions during cyber deception tasks	Small sample limits generalization
Moody *et al.*	2018	Model based on neuroevolutionary algorithms mimicked effects of bounded rationality on security investment choices	Simplistic abstraction of complex organizational factors
Rusch *et al.*	2018	Proposed using neuro-cognitive metrics from simulation training to identify personnel resilient to cyber threats	Awaiting practical testing validation
Krajbich *et al.*	2014	Proposed model of cybercriminal motivations based on neural risk/reward circuits	Hypothetical neural links require empirical testing
Mrdjenovich *et al.*	2018	Neurofeedback training improved working memory performance and reduced cyber errors	Possible demand characteristics from lack of control condition
Mrdjenovich	2018	Implications of neuroeconomics risk research for cybersecurity policy and technology design proposed	Hypothetical applications need empirical testing
Rao *et al.*	2018	Computational model simulated prefrontal cortex role in strategic cyber deception	Simplified model needs empirical grounding
Acquisti *et al.*	2017	Highlighted potential of neuroeconomics insights like dual process thinking to enhance privacy nudging	Awaiting large-scale field applications
Hibshi *et al.*	2017	Eye-tracking demonstrated increased visual attention to security warnings during cognitively depleted states	Limited ecological validity of lab studies
Anderson *et al.*	2016	FMRI study revealed neural reactions to fear appeals versus gain framing for security messages	Further research on message tailoring needed
Leykin *et al.*	2016	Neural evidence from cyber simulation confirmed dual process theories distinguishing reflexive versus reflective responses	Limited task realism
Teper *et al.*	2015	FMRI confirmed emotions like anger and anxiety linked to reduced concern for cyber ethicality	Did not explore interventions to strengthen moral cognition
Nurse *et al.*	2014	Proposed neuroeconomic framework using EEG for modeling insider threat behaviors	Limited validation with real cyber contexts
Dancy	2013	Outlined implications of neuroscience deception research for cyber behavioral modeling	Awaiting integration and testing with technical systems
Riedl and Javor	2012	Hyperscanning EEG revealed increased theta synchronization during cooperative cyber tasks	Limited sample size and task realism

3. Theoretical Frameworks

Numerous significant theoretical frameworks based on the biology of human decision-making are provided by neuroeconomics which can showcase fresh insights into persistent cybersecurity problems. These theories provide added variables and interactions to models of cyber hazards and resilience by bringing forward certain neurological systems and psychological processes that undermine decision-making, behaviour, and choice to further strengthen cybersecurity research and practice (Kritika, 2023), some of the most pertinent ideas from the neuroeconomics literature will be briefly introduced in this part along with an explanation of their possible uses.

3.1 Dual Process Theory

One of the most influential theories to come out of behavioral economics and cognitive psychology, which served as a springboard for the neuroeconomic study of human cognition and decision-making, is dual process theory (Grayot J.D, 2020). Human cognition contains two primary processing modes that function in parallel, as extensive research has shown (Kahneman, 2011; Evans & Stanovich, 2013). Fast, instinctive, intuitive thinking also known as System 1 allows for quick decisions and judgments based on feelings, intuition, and heuristics whereas System 2 calls for more careful, slower thinking that requires concentration and effort. Several seeming inconsistencies and cognitive biases in human decision-making and judgment are explained in part by the interplay between these two categories of processes.

Investigating the cognitive biases and actions associated with cybersecurity is made much easier by the dissimilitude between automatic and regulated thinking where emotional reactions and gut feelings that don't prompt thorough System 2 risk appraisal are the main causes of vulnerability to phishing emails and social engineering. System 2 vigilance might become weary due to cognitive strain from information overload and complicated security requirements, which makes users depend more heavily on mistake-prone System 1 decisions (Chen & Cho, 2020). An individual's present cognitive state and the relative dominance of automatic vs controlled thinking may be detected using neuroeconomic methods such as EEG, which evaluate the speed at which information is processed. Depending on a user's current attentional capacity and propensity for automatic judgment, this might be utilized to dynamically customize security interfaces or awareness training.

Research on reducing the status of and encouraging deliberate decision-making may represent chances to improvize security practices by entailing human cognition into two different ways of processing information: a more laborious, analytical "System 2" and an automatic, intuitive "System 1" (Tsohou et al., 2015). System 2 processes information more deliberately but is restricted by cognitive resources whereas System 1 is more efficient though prone to cognitive biases. The brain foundations of different processing modes have been clarified by neuroeconomic studies, which link the prefrontal cortex to controlled, analytical thinking and the amygdala and striatum to automatic emotive reactions (Satpute & Lieberman, 2006).

Those who want to "nudge" people toward safer online conduct should purposefully use System 2 processing at pertinent decision points. Interventions could involve temporal delays or cognitive load manipulations prior to security-critical actions, structuring security prompts or warnings to facilitate analytical processing, or using cognitive strain or depletion to temporarily downregulate effortful System 2 processing. By grounding intervention strategies in a neurocognitive framework of dual-process decision-making, cybersecurity initiatives can harness the complementary strengths of intuitive and analytical processing modes, circumventing the limitations of relying solely on explicit mandates or rational appeals (Kritika, 2024).

3.2 Prospect Theory

Prospect theory is one of the most important models in behavioural economics, supported by a wealth of empirical data from neuroeconomic studies (Fox & Poldrack, 2009). According to the theory, rational agents base their judgements on subjective assessments that are contextualized in respect to a reference point, rather than objectively weighing costs and benefits (Kahneman, 2011). The preliminary focal point holds that people feel the potential loss disproportionately than similar reward which is attributed to the conceptualization of loss aversion. The enhanced brain reaction to possible losses is supported by neuroimaging studies that use functional magnetic

resonance imaging (fMRI), which show higher activity in the striatum and amygdala areas when faced with potential losses (Tom et al., 2007).

It directly applies to decision-making situations in cyberspace, where assessing anticipated costs against potential advantages is a common practice. According to the notion, mandatory security measures like strict password restrictions will be viewed much more negatively. Another area where people erroneously overvalue possible losses from data sharing in contrast to similar advantages is privacy. Adoption and impact could be increased by carefully drafting cyber laws and incentives to take loss aversion into consideration with regard to reference points and aids in explaining the unusual actions, such as people taking unnecessary risks in order to avoid admitting to little losses, a practice similar to hiding data breaches. The study shows how this theory, which is supported by neuroeconomic data, may be used in decision-making process in cyberspace. The foundational idea, i.e., loss aversion provides a framework for comprehending and resolving people's disproportionate aversion to perceived losses. This aversion can appear in a variety of cybersecurity scenarios, such as risk-taking behaviours, resistance to security measures, and privacy concerns.

3.3 Intertemporal Choice

An elemental contradiction that prevails between neurological systems that promote spontaneous satisfaction and long-term consideration has been identified, seen in a number of cyber decision-making fields, such as postponing software patches or security updates in order to minimise short-term inconveniences even in the face of increased long-term dangers. Strongly activated in response to current incentives, the ventral striatum becomes less active in response to future opportunities (McClure *et al.,* 2004; Schweighofer *et al.,* 2008). In contrast, when reward delays rise, the lateral prefrontal cortex and related regions show prolonged engagement, which may indicate the activation of cognitive control mechanisms to counteract impulsive inclinations. The conflict prevailing between immediate and delayed gratification, offering valuable understanding of temporal discounting biases having significant ramifications for comprehending and preventing less-than-ideal cyber choices that are motivated by excessive present-orientation is represented by dissociation of brain. Security policies being broken for expediency against long-term cyber hazards tends to intricate the situation where the war between present and future goals is evident. Due to the preference for short-term expenses over long-term gains, investments in enhanced security infrastructure or cultural transformation may not be optimized (Takahashi, 2009). A potential path for improvement based on neuroeconomic insights is to better match security messages and incentives with human intertemporal preferences. In fact, identifying people who are more likely to engage in these dangerous cyber behaviour may be aided by measuring brain indicators of short-term reward sensitivity. Even though intertemporal choice is still a critical component of human decision-making, current neuroeconomic models of it offer a solid platform for research.

3.4 Social Decision-Making

Due to our innate social nature, humans have developed choice architectures and motives that defy individualistic notions. Using techniques like fMRI and transcranial magnetic stimulation, neuroeconomics has thoroughly mapped social cognition and decision circuits to investigate dynamics like trust, collaboration, and justice (Rilling & Sanfey, 2011). The brain areas associated with theory of mind and empathy, which underpin strategic social reasoning, have been identified as key results (Van Overwalle, 2009). Neural foundations for social behaviour observation learning are provided by the brain's mirror neuron system (Iacoboni & Dapretto, 2006). Research also shows that different networks are active in cooperative versus competitive situations (Decety *et al.,* 2004).

These social motivations and biases are integral to cyber contexts involving distributed users and high coordination costs. Employees often mimic behaviors of coworkers regarding security compliance, and social norms help dictate acceptable risk-taking (Serra, 2021). Adversaries exploit human social tendencies through strategies like phishing. Neuroeconomic research on motivations behind insider threat behaviors also points to distorted social incentives within organizations as a key factor (Nurse *et al.,* 2014). Better incorporating validated neural models of social cognition could strengthen game theoretic and agent-based simulations of cyber interactions among various actors.

The complex social dynamics enabled by modern IT systems warrants deeper exploration through neuroeconomic frameworks of social decision architectures in the human brain.

3.5 Framing Effects

The way choices are framed through language, context, or presentation format can profoundly influence decisions, even when objective costs and benefits remain fixed. Seminal prospect theory research by Kahneman and Tversky illustrated this effect in human judgment and cognition (Kahneman & Tversky, 1981). Neuroimaging confirms that different frames activate distinct neural pathways related to either risk-seeking or risk-averse behaviors (De Martino et al., 2006). Because human psychology is hardwired, such framing effects hold true across situations and cultures (Levin et. al., 2014).

The framing phenomenon affects cyber choice scenarios, as prospect theory demonstrates. Motivation can be increased by gain-framed appeals, but attention can be reduced by warnings that are interpreted as carrying disproportionate dangers. The propensity of sharing of data is reduced when decisions based on privacy are framed in terms of losses. Though evidence points to the involvement of brain areas related to emotional processing and value calculation, the exact neurological processes behind framing effects remain unclear. Gain-framed appeals and a reduction in loss-aversive language are two ways that neuroscientific knowledge might improve cybersecurity marketing and policy. Neuroeconomic research can also help with the creation of data-sharing guidelines and privacy frameworks (De Martino et al., 2006).

4. Neuroeconomic Factors in Cybersecurity Behaviors

Research in neuroeconomics and cybersecurity has amicably thrown light on how human decision-making influences risk and resilience. Risk perceptions, intertemporal biases, emotional effects, social incentives, and cognitive limitations are important neuroeconomic factors. These factors impact decision-making, feelings, and actions, providing insight into user, supervisory, and hostile behavior in virtual environments (Chen, 2019). The evaluation and first incidence response to dangers is a core aspect of cybersecurity which includes neurological circuits such as the insula, prefrontal cortex, and amygdala. Cybersecurity choices with postponed costs or rewards are under the topic of intertemporal choice, which involves weighing immediate vs later results. Temporal discounting biases can be explained mechanistically by neurological dissociation, which might show up as putting off software patches or security upgrades to prevent short-term difficulties even while they increase long-term risks. The brain substrates involved in processing emotions and making decisions is influenced by social incentives and peer pressure which is hampered by the cognitive limitations, such as poor working memory and attention spans, which can make an individual more susceptible to online attacks. It is possible to create more effective techniques to encourage safe cyber behaviors and reduce vulnerabilities resulting from the inherent limits and biases of human decision-making by firmly establishing cybersecurity research in neuroscience-based models of human psychology (Kritika, 2024). The phenomenon of neuro-ethics (Kritika, 2024) also play a vital role in decision making process to ensure that the decision is ethically in terms of the process.

4.1 Risk Perceptions and Biases

A biological viewpoint on human risk assessment is provided by neuroeconomics, which demonstrates how cognitive shortcuts and biases cause human motives and behaviors to frequently diverge from realistic probability when it comes to avoiding cyberthreats. A core result in neuroeconomics is loss aversion, a phenomena characterized by over-aversion to unlikely losses, over-weighting of novel hazards, and indifference for abstract concerns (Tom *et al.,* 2007). It shows that the striatum and amygdala, two emotion and reward areas, are disproportionately activated by potential losses, which causes a disproportionately negative effect on one's mood. This may show up as overreaction to cyber-events, including data breaches, in comparison to privacy safeguards. A scientific basis for unreasonably loss-averse cyber activities can be found in neuroimaging findings of enhanced brain reactions to losses (Yacubian *et al.,* 2006). A crucial component in the limbic system that plays a pivotal role in processing emotional salience and threat detection, exhibits a robust response to potential gains, marks the attenuated response to losses.

According to neuroeconomic research, people frequently overestimate risks with low probability and underestimate those with intermediate to high probabilities. This phenomenon causes people to become disproportionately anxious about new cyberthreats (Hsu *et al.,* 2005). In insurance decision scenarios, when security considerations are frequently disregarded, this tendency is clearly visible. According to Wittmann *et al.* (2008), fMRI neuroimaging studies show that novelty increases brain responses to danger by activating the amygdala and ventral striatum. However, this impact quickly becomes accustomed, which may be a factor in the disproportionate anxiety elicited by new cyberthreats (Kostyuk & Wayne, 2021). Certain biases in people's opinions are revealed by neuroeconomic insights, and brain indicators of novelty reactions or loss aversion can be used as biomarkers to measure these biases in different persons. While there is a dearth of direct neuroeconomic cybersecurity research, our understanding of the neurobiology of risk cognition provides important new perspectives that might improve cyber risk assessment and mitigation strategies. Training techniques that employ novelty-based attentional capture or differential probability weighting may be used to enhance threat awareness and encourage more accurate risk assessments.

4.2 Intertemporal Biases and Delayed Gratification

Short-term gains and long-term protection are usually traded off in cybersecurity. Workers get around security to save time, and when rapid product releases are prioritised above well-written code, technical debt mounts. A biological perspective on such intertemporal choices is provided by neuroeconomic research. According to fMRI research, the striatum and other limbic system regions closely monitor immediate rewards, but the lateral prefrontal cortex is more active when considering future events (McClure *et al.,* 2004). This disparity contributes to the explanation of why people choose smaller, sooner rewards over bigger, later ones. According to Margittai *et al.* (2018), cortisol is a hormone that also increases striatal responses to immediate rewards while decreasing prefrontal activity. This suggests that neurochemicals have a role in intertemporal decision.

It is evident that these neurobiological causes of impatience and present bias affect online decisions and actions. Instead of adhering to security best practices which provide delayed protection, employees concentrate on short-term productivity improvements often prioritize short-term savings, managers underinvest in significant infrastructure investments. It may be possible to forecast higher risk employees by identifying neurological and endocrine indicators of people's time discounting inclinations by scanning or hormone levels. Neuroeconomics models provide possible direction for framing security policy and training to utilize cognitive processes in the frontal lobe. Additionally, studies indicate that cognitive load makes impatient tendencies in intertemporal choices even worse (Hinson *et al.,* 2003). Thus, heavy workloads may reduce cyber alertness by wearing out self-control, emphasising the need for security automation and streamlined procedures.

While direct cybersecurity applications are still a ways off, current theory-driven factors regarding the brain drivers of short-termism offer a means to include them into models that predict issues related to delayed gratification that are applicable to many cyber scenarios. In the absence of further confirmation, methods evaluating personal discounting inclinations can present themselves as viable instruments for labour screening. For research integrating neuroeconomic intertemporal choice frameworks into cybersecurity scholarship and practice, this aspect of human cognition is a major focus in the near future.

4.3 Social Preferences and Cooperation

Social dynamics among connected users are inherently involved in modern cybersecurity, and they must work together to preserve shared information resources. However, self-centeredness frequently thwarts group decisions and actions that minimize cyber risk. Important biological insights into human social decision-making that are applicable to cyber settings are provided by neuroeconomic research. Research that simultaneously assess brain activity in several people using hyper scanning EEG elucidate the critical functions that theta band synchronization plays in promoting social coordination (Dikker *et al.,* 2017). During cooperation activities, there is an experimental increase in individualistic decisions when this neurophysiological system is disrupted. This method shows the neuronal drivers of group synergies that are important for cooperative cyber norms and regulations. Neuroeconomic

knowledge may be used to parameterize game theoretic models that study how network topologies affect how people choose to take collective cyber risks.

According to Greene and Paxton (2009), brain imaging has revealed neural patterns linked to antisocial behaviors including injustice and dishonesty. This might be seen as a brain signal for taking revenge. Cyber cooperation results may be predicted via a fresh lens by modeling the balance between prosocial and antisocial neurobiological impulses, controlled by group membership and incentives. Hormone assays are complementary tools that can help identify cyber professionals who are more likely to have negative social interactions while under stress.

The study of human sociality and neuroeconomics has great potential to further cybersecurity studies on adversarial and collective dynamics. A paradigm for forecasting cooperative dynamics in cyber settings that are influenced by variables like group membership and incentive structures (Rilling & Sanfey, 2011). Complementary techniques may augment these neural markers by assessing physiological correlates of stress reactivity and their potential impact on social decision-making in cyber personnel whereas direct applications remains speculative (Mehta & Josephs, 2010), they highlight the potential value of integrating neuroscientific perspectives to advance models of human behaviour in cyber domains.

4.4 Emotions and Stress Responses

Emotional state has well-documented implications on decision-making and behaviour relevant to cyberspace. Important brain circuits such as the amygdala, ventral striatum, and certain neurotransmitters that regulate emotional influences over decision-making and risk-taking have been identified by neuroeconomic research (Lerner et al., 2015). According to Preston *et al.* (2007), FMRI studies demonstrate that increased activity in these emotion areas impairs executive functions and cost-benefit calculations. According to Yu (2016), exposure to stress triggers sympathetic nervous system reactions that also affect prefrontal cognition.

These brain circuits contribute to the understanding of why emotional responses to cyber-events can supersede analytical reasoning. Fear produced by events such as data breaches leads to automatic reactions that overlook trade-offs. Anger after cyberattacks leads to revenge that disregards the repercussions. Attentional control and situational awareness are weakened by the stress that demanding cyber positions place on employees. Methods for evaluating the brain activity patterns, stress hormone levels, or autonomic physiology could potentially quantify an individual's current emotional state to customize cyber training and communication approaches accordingly.

Improved cyber decision-making is based on neurochemical systems linked to the emotional regulation of cognition also shows promise. Guanfacine is one example of an alpha-2 agonist drug that reduces emotion-driven biases and impulses by strengthening prefrontal processes and dampening mygdala reactivity (Mueller *et al.,* 2010). By addressing the neurological underpinnings of cyber decisions directly, such neuropharmacological strategies informed by neuroeconomic research present novel avenues for enhancing cyber decisions. Although this field of study is still in its infancy, neuroeconomic concepts and assessment instruments that distinguish emotional influences on judgment show great promise for understanding how emotions drive both beneficial and harmful cybersecurity behaviors. This provides avenues anchored in neuroscience to further the modeling, tracking, and regulation of these commonplace human events, moving beyond the use of self-reports.

4.5 Cognitive Limitations and Heuristics

The cognitive ability of humans to process and comprehend information is limited. The brain systems such as the lateral prefrontal cortex and basal ganglia that determine mental bandwidth restrictions and consequent reliance on mental shortcuts are characterized by neuroeconomic research (Huettel *et al.,* 2014). These cognitive constraints contribute to the explanation of why cyber training overload frequently backfires: working memory constraints hinder the absorption of too many security regulations. Additionally, using inadequate choice heuristics is amplified by cognitive strain. Workers might, for instance, choose options based only on feelings of safety rather than doing an analytical risk assessment, relying instead on the affect heuristic (Kusev et al., 2017). These heuristics and capacity restrictions, which are disclosed by neuroeconomic techniques, reflect important limitations on the quality of human cyber decisions.

One way to optimize information flow for security situations without going beyond user cognitive constraints is to use neuroimaging techniques that measure working memory loads (Borst *et al.,* 2010). Even the selection of candidates for cognitively demanding cyber professions may be aided by neural efficiency scores. According to research, organized therapies such as mindfulness meditation improve metacognition and prefrontal executive processes that are linked to heuristic biases (Mrazek *et al.,* 2013). Using such neuroscience-based cognitive improvement strategies could improve threat assessment and cyber workforce awareness. Similar to this, neuroeconomic insights on restricted cognition highlight the importance of automation and nudging to mould cyber behaviour within the cognitive limitations of humans. Smart defaults and framing can direct decisions without necessitating complete analytical engagement (Thaler & Sunstein, 2009). Research on cyber deception also shows that automated threat detection works better than sluggish reasoning in catching spear phishing tactics. Aligning policies and architectures to human bandwidth boundaries through neuro-economically-informed models offers much potential.

While neuroimaging and cognitive assessment methods require additional validation, neuroeconomics already provides well-established theoretical frameworks on the psychology of limited cognition highly relevant for evolving cyber risk and resilience models. Much potential exists in translating these insights into design principles and workforce selection approaches as cyber decision burdens continue growing.

5. Potential Applications

While still an emerging research domain, the synergistic fusion of neuroeconomic concepts and techniques with cybersecurity questions holds immense promise for catalyzing scientific and practical advances. This section will review near-term possibilities for applying neuroeconomic frameworks and measurements to further four key applied problem spaces in cybersecurity: 1) Enhancing security awareness training and interventions; 2) Optimizing the design of cyber policies and incentives; 3) Improving insider threat detection through neurobehavioral modeling; and 4) Engineering human factors insights from neuroscience into security technologies. For each area, relevant foundational work will be summarized and specific guidance emerging from neuroeconomic research will be proposed. Significant opportunities exist for assimilation of neuroeconomic human decision-making expertise into both cybersecurity scholarship and practice.

5.1 Improving Security Awareness Training and Interventions

Organizational resilience is essentially determined by employee motivation, attitudes, and cybersecurity awareness. Research, however, demonstrates that frequently required security trainings, which overwhelm users with numerous regulations and easily forgotten alerts, are ineffective (Cox, 2012). Such technical training is frequently counterproductive, as evidenced by neuroeconomic insights on working memory constraints, attentional limits, and dual process cognition. Instead, the application of behavioral economics and neuroscience principles highlights the use of training that is minimalist and consistent with daily activities and internal mental models in order to convey the fundamental "why" behind security regulations (Bravo-Lillo *et al.,* 2013).

In neuroeconomic research, temporal framing effects also demonstrate that messages emphasizing immediate costs or rewards are more effective in motivating people than delayed consequences due to temporal discounting biases. Citing abstract concerns is not as significant as communicating specific, proximate hazards like account theft like economic espionage which feel temporally remote (Acquisti, 2017). Emotionally salient images and cases also better engage neural attention systems compared to technical descriptions or writtens directives according to brain imaging studies (Anderson *et al.,* 2016). Measurement techniques like eye-tracking, pupillometry, and EEG provide additional metrics to quantify user engagement and comprehension during security trainings based on neurocognitive models. Real-time neural feedback could optimize delivery pacing and content density tailored to recipients' current attentional state and situational demands. Even periodic scanning via fMRI could map evolving mental models regarding security threats and norms for more personalized intervention.

Therefore, neuroeconomic insights present a huge opportunity to advance an empirically supported human-centered paradigm for security awareness training that emphasizes neurocognitive principles above repetitive technical detail memorization. Training personalization and efficacy will be further enhanced by the ongoing

integration of neuroscience-based validated approaches monitoring attention, emotions, and mental bandwidth limits.

5.2 Tailoring Cybersecurity Policies and Incentives

Security policies plays a pivotal role and human judgment about the compliance makes them noteworthy. The traditional frameworks such as deterrence often encounter difficulties due to prejudice and neglect in monitoring and punishment. The theory of prospect biases and intrinsic social inclinations must be taken into consideration in order to enhance policy framing and motivating techniques. New security rules should prioritize possible loss aversion opportunities above new obligations in order to encourage buy-in. Due to temporal discounting effects, quick punishments or the withdrawal of incentives have greater deterrent power than delayed punishment (Sayegh *et al.,* 2017). Punitive fines are not as effective in eliciting collaboration as group-based incentives that take use of conformity inclinations and social learning neuroscience models (Cui *et al.,* 2022). Putting faces and names to cybersecurity authorities can improve social accountability because of the brain's neurological sensitivity to human interactions. Emerging applications of neuroeconomic games measuring trust, cooperation, and reactions to norm violations show particular promise for screening personnel prone to risky cyber behaviors based on neural marker. The ongoing integration of realistic models of human motivations from neuroeconomics will further advance the efficacy and ethics of cybersecurity strategies.

5.3 Detecting Insider Threats via Neurobehavioral Modeling

Among the most dangerous and unmanageable cybersecurity threats are those caused by malicious insiders with authorized access. Excessive false alarms are a common cause of traditional controls failing. Insider threat detection can be enhanced by additional variables relating to distorted threat perceptions, poor impulse control, and anti-social tendencies, which are being discovered through research in the fields of social neuroscience and neuroeconomics.

A groundbreaking neuroeconomic approach builds models to identify abnormal neurobehavioral patterns indicative of internal espionage by using EEG monitoring during cybersecurity scenario activities (Nurse *et al.,* 2014). Assessing stress hormone levels holds potential in determining a person's vulnerability to social influences that facilitate insider threats. In tests, brain stimulation using transcranial magnetic stimulation to improve moral judgments has shown effectiveness in lowering intents to break cyber regulations (Teper *et al.,* 2011). Continued study can improve neurological and biometric signatures that precede insiders' unethical cyber actions for incorporation into personnel screening and access control systems. Similar brain indicators of skewed social choices suggestive of possible insider compromise are shown by neuroeconomic game paradigms. Neuro-policy research, which combines ethical analysis and neuroscience insights, offers crucial help on finding a compromise between insider threat identification and privacy and fairness issues (Uljin *et al.,* 2022). Carefully tested neurobehavioral monitoring systems based on neuroeconomic social decision-making models provide great unfulfilled potential as an extra layer of socio-technical defenses against insider cyber threats.

5.4 Accounting for Human Factors in Security Designs

Neuroeconomic principles have the ability to optimize cyber infrastructures and technologies by taking into account human capabilities and limits, rather than just technological priorities. This goes beyond training and incentives. A neuroergonomic approach to human factors, usability design that makes use of affordances, restrictions, and natural mapping derived from mental models enhances adoption and reliability (Rajivan & Camp, 2016). Bounded cognition is also not as taxed by interfaces that automate routine operations and simplify sophisticated technological controls.

Dual process thinking research emphasizes the importance of system defaults and subtle cues that direct instinctive reactions in order to heighten awareness and enhance cyber hygiene (Acquisti et al., 2017). Neuroscience findings on fundamental human motivations beyond consequences and commands are similarly leveraged by design

elements that evoke emotional involvement or social motivations for protection. Virtual simulations based on theories of neurocognition concepts of situated learning and embodied cognition offer immersive training environments as well (D'Amico & Whitley, 2007). The virtual setup of neurodesign thinking illustrate initial pathways for assimilating neuroeconomic insights on human behavior, emotions, and mental processes into user-centered security principles and architectures, uncovering the neuroeconomics into cyber contexts will enhance fit and adoption of policies, training, and technologies. Ongoing collaboration between neuroscience, cybersecurity, ethics, and design researchers offers much promise in uniting biological and social considerations into human-centered security.

6. Limitations and Ethical Considerations

Although there is much promise in the nascent confluence of neuroeconomic principles with cybersecurity problems, there are still significant limitations and unanswered ethical questions that call for caution as this field grows. Concerns of validity, privacy, permission, and unintentional effects arise when applying neuroeconomic insights for security prediction or intervention, as they do with any interdisciplinary application of complex bio-behavioural data. This part will go over the main limitations of the neuroeconomic research that is now available for cyber settings, as well as the major ethical concerns that need to be addressed in advance by proactive policy planning. It will be ensured that this potentially transformative convergence strengthens rather than weakens key security and societal values by navigating such problems in an open, evidence-driven manner.

Small sizes of available data and simplified laboratory activities are used in the majority of neuroeconomic studies, raising concerns about the generalizability and ecological validity. Large-scale randomized trials that are required to reliably quantify the effect sizes of neuro-markers on cyber-relevant outcomes are typically not feasible due to the high costs of FMRI. Before being relied upon in real-world scenarios, biomarkers such as neural activity patterns during cybersecurity games need to undergo comprehensive validation, even though they initially show promise in detecting insider threat behaviors (Nurse *et al.,* 2014). Instead of objectively assessing predictiveness for applied use, this runs the risk of overinterpreting noisy neuroimaging data based on confirmation bias if sufficient safeguards are not in place.

Neuroeconomic models might potentially fall short in simulating intricate real-world decisions including wider social or cultural contexts outside of the laboratory. Moral principles and organizational responsibilities that go well beyond personal cognitive processes are involved in cyber decisions. Combining the propensity for cybercrime with lab neuro-predictors raises ethical and scientific concerns that sought to supplement comprehensive behavioural cybersecurity tactics. Additionally, there are justifiable worries that increment in neuro-monitoring can potentially work against core cybersecurity motives by eroding employee discretion or trust (Uljin *et al.,* 2022). Unintentional counterproductivity can arise from relying too much on neuro-surveillance rather than culture cultivation. Neuroeconomic monitoring needs to be used with caution in situations where the advantages outweigh the hazards to an individual's rights and the culture of the company, just like any other biometric approach.

Proactive responses to the policies are necessary in light of the ethical concerns raised by the emergence of neuroscience applications in security contexts (Tennison & Moreno, 2012). People are becoming more hesitant to use body scanners and biometric surveillance because they worry about consent violations and privacy invasion. Without intentional safeguards, the use of brain biomarkers or neuroimaging for danger screening could come under much more criticism. Additionally, there is a chance that security improvements will be overstated before data supporting predictive neuro-markers is gathered, leading to an early implementation that unfairly burdens vulnerable populations due to public anxiety.

It is also necessary to examine and impose restrictions on the possibility of governments or companies forcing cognitive improvement or emotion management under the pretext of security. Without ethical rules, military research on pharmaceutical substances to improve soldier focus or reduce anxiety clearly has room for abuse. Neural security approaches, depending on institutional monitoring and incentives, may facilitate manipulation rather than empowerment. Before neuroscience becomes a cybersecurity magic bullet, clear policies governing appropriate use and subjects' rights are needed. Given the discrepancies in public views of brain imaging insights and scientific validity, establishing legal criteria for neuro-based evidence in courts or security programs is still difficult (Jones *et al.,* 2013). Guidance is necessary for judges and other officials to avoid cognitive biases while evaluating

neuroeconomic testimony. Additionally, there's a chance that malicious software may reverse engineer neural models to exploit rather than strengthen security. Advancing neuroeconomics-based cyber defenses must occur alongside adversary neuroscience foresight to ensure societal resilience.

7. Conclusion

The paper forecasts the way in which neuroeconomic concepts might strengthen the realm of cybersecurity by building a foundation in sagacious human psychology and biology models, before they can be widely adopted, though, excitement needs to be controlled with strict validation and moral considerations. Evidence from neuroscience should supplement rather than replace comprehensive cyber policies that emphasize culture, skills, and incentives. Researchers from different fields, such as neuroscience, cybersecurity, law, and ethics, can consciously share knowledge to improve our understanding of the human element that underlies risks and resilience.

This literature review concludes by highlighting neuroeconomics as an intriguing multidisciplinary study area with a wide range of potential applications to cybersecurity advancement. The basis for more detailed explanations of the behaviour of users, managers, and hackers is provided by current theories and brain metrics. Cyber risks can arise due to the complication of decisions made by humans be it emotionally or due to certain social conditions which nevertheless can be decreased by meticulous cooperation across several domains. But active governance is required to ensure ethical use and integration with comprehensive cyber policies. Cybercrimes are generally caused by the mind and its limitations; understanding neuroeconomics may help to shed light on this human component.

8. Future Scope

The literature review showcases the noteworthy potentiality for neuroeconomic theories and methods to bolster research and practice in cybersecurity. However, more interdisciplinary collaboration is needed to validate and responsibly apply neuroscientific insights in complex organizational contexts. Table 3 highlights the potential research questions to be addressed in the future.

Table 3. Probabilities for future research arena

S.no.	Research Question
1.	How can neuroeconomic concepts like prospect theory and framing effects be applied to improve employee security training programs and interventions?
2.	What neurophysiological markers measured via EEG or fMRI are most predictive of insider threat behaviors and can enhance early detection models?
3.	How do emotion regulation techniques guided by neuroeconomic research affect risk-taking behaviors and ethical decision-making in simulated cyber tasks?
4.	Can neuroeconomic studies on intertemporal choice provide insights on the biological drivers of impatience and short-termism undermining cybersecurity investments?
5.	How do different incentive structures grounded in neuroeconomic research on reward systems affect employee security compliance and organizational resilience?
6.	Can neuroimaging techniques like fMRI quantify the effects of cognitive load manipulations on cyber situational awareness and judgement biases?
7.	How do neural markers of emotions like anxiety or anger identified through real-time EEG monitoring affect defensive behaviors in simulated cyber response scenarios?
8.	What neuroethical guidelines and oversight systems are needed to balance the promise and perils of "neurosecurity" techniques in applied settings?
9.	How can neuroergonomic principles strengthen the usability and adoption of security technologies by aligning interface design with realistic neural and cognitive constraints?

10.	What policy frameworks are required to enable effective and ethical translation of validated neuroeconomic insights on human decision-making into improved cybersecurity strategies?

References

Bokhari, S.H., Wahab, A., Malik, H., Ahmad, J., & Lee, M. (2020). Deep neural network model based on eeg for cybersecurity insider threats detection. Scientific Reports, 10(1), 1-10.

Borst, J.P., Taatgen, N.A., & Van Rijn, H. (2010). The problem state: A cognitive bottleneck in multitasking. Journal of Experimental Psychology: Learning, Memory, and Cognition, 36(2), 363-382. https://psycnet.apa.org/doi/10.1037/a0018106

Brinton Anderson, B., Vance, A., Kirwan, C.B., Eargle, D., & Jenkins, J.L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. European Journal of Information Systems, 25(4), 364-390. https://doi.org/10.1057/ejis.2015.21

Camerer, C., Loewenstein, G., & Prelec, D. (2005). Neuroeconomics: How neuroscience can inform economics. Journal of Economic Literature, 43(1), 9-64. https://doi.org/10.1257/0022051053737843

Chen, J.Q. (2019). A Strategic Decision-Making Framework in Cyberspace. IGI Global, 12. https://doi.org/10.1037/14322-003

CISCO. (2008). Data leakage worldwide: The high cost of insider threats.

Dikker, S., Wan, L., Davidesco, I., Kaggen, L., Oostrik, M., McClintock, J., Rowland, J., Michalareas, G., Van Bavel, J.J., Ding, M., & Poeppel, D. (2017). Brain-to-brain synchrony tracks real-world dynamic group interactions in the classroom. Current Biology, 27(9), 1375-1380. https://doi.org/10.1016/j.cub.2017.04.002

Fehr, E., & Rangel, A. (2011). Neuroeconomic foundations of economic choice—recent advances. Journal of Economic Perspectives, 25(4), 3-30. https://doi.org/10.1257/jep.25.4.3

Fox, C.R., & Poldrack, R.A. (2009). Prospect theory and the brain. Neuroeconomics, 145-173. https://doi.org/10.1016/B978-0-12-374176-9.00011-7

Glimcher, P.W., & Fehr, E. (2013). Neuroeconomics: Decision making and the brain. Academic Press.

Grayot, J.D. (2020). Dual process theories in behavioral economics and neuroeconomics: A critical review. Review of Philosophy and Psychology, 11(1), 105-136. https://doi.org/10.1007/s13164-019-00446-9

Greene, J.D., & Paxton, J.M. (2009). Patterns of neural activity associated with honest and dishonest moral decisions. Proceedings of the National Academy of Sciences, 106(30), 12506-12511. https://doi.org/10.1073/pnas.0900152106

Hayashi, Y., & Tahmasbi, N. (2020). Decision-making process underlying bystanders' helping cyberbullying victims: A behavioral economic analysis of role of social discounting. Computers in human behavior, 104, 106157. https://doi.org/10.1016/j.chb.2019.106157

Hinson, J.M., Jameson, T.L., & Whitney, P. (2003). Impulsive decision making and working memory. Journal of Experimental Psychology: Learning, Memory, and Cognition, 29(2), 298-306. https://psycnet.apa.org/doi/10.1037/0278-7393.29.2.298

Hsu, M., Bhatt, M., Adolphs, R., Tranel, D., & Camerer, C.F. (2005). Neural systems responding to degrees of uncertainty in human decision-making. Science, 310(5754), 1680-1683. https://doi.org/10.1126/science.1115327

Huettel, S.A., Stowe, C.J., Gordon, E.M., Warner, B.T., & Platt, M.L. (2006). Neural signatures of economic preferences for risk and ambiguity. Neuron, 49(5), 765-775. https://doi.org/10.1016/j.neuron.2006.01.024

IBM. (2019). IBM security report: Cost of a data breach report 2019. Computer Fraud & Security, 2019(8). https://doi.org/10.1016/S1361-3723(19)30081-8

Jones, O.D., Wagner, A.D., Faigman, D.L., & Raichle, M.E. (2013). Neuroscientists in court. Nature Reviews Neuroscience, 14(10), 730-736. https://doi.org/10.1038/nrn3585

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American Economic Review, 93(5), 1449-1475. https://doi.org/10.1257/000282803322655392

Kahneman, D., & Egan, P. (2011). Thinking, fast and slow. Farrar, Straus and Giroux, 1.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk Handbook of the Fundamentals of Financial Decision Making, 99-127. https://doi.org/10.1142/9789814417358_0006

Klucharev, V., Hytönen, K., Rijpkema, M., Smidts, A., & Fernández, G. (2009). Reinforcement learning signal predicts social conformity. Neuron, 61(1), 140-151. https://doi.org/10.1016/j.neuron.2008.11.027

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. Journal of Global Security Studies, 6(2), ogz077. https://doi.org/10.1093/jogss/ogz077

Krajbich, I., Oud, B., & Fehr, E. (2014). Benefits of neuroeconomic modeling: New policy interventions and predictors of preference. American Economic Review, 104(5), 501-506. https://doi.org/10.1257/aer.104.5.501

Kritika (2024). A review on harmonizing psychological factors into cyber space. International Journal of Scientific Research in Network Security and Communication, 12(2), 11-18

Kritika, M. (2024). A comprehensive study on navigating neuroethics in Cyberspace. AI and Ethics, 1-8. https://doi.org/10.1007/s43681-024-00486-7

Kritika. (2023). Demystifying Cyber Crimes. IGI Global.

Kusev, P., Purser, H., Heilman, R., Cooke, A.J., Van Schaik, P., Baranova, V., Martin, R., & Ayton, P. (2017). Understanding risky behavior: The influence of cognitive, emotional and hormonal factors on decision-making under risk. Frontiers in Psychology, 8, 102. https://doi.org/10.3389/fpsyg.2017.00102

Lerner, J.S., Li, Y., Valdesolo, P., & Kassam, K.S. (2015). Emotion and decision making. Annual Review of Psychology, 66, 799-823. https://doi.org/10.1146/annurev-psych-010213-115043

Levin, I.P., McElroy, T., Gaeth, G.J., Hedgcock, W., & Denburg, N.L. (2014). Behavioral and neuroscience methods for studying neuroeconomic processes: What we can learn from framing effects. American Psychological Association, 43–69. https://psycnet.apa.org/doi/10.1037/14322-003

Margittai, Z., Nave, G., van Wingerden, M., Joëls, M., Schwabe, L., & Kalenscher, T. (2018). Glucocorticoids dissociably modulate prefrontal and hippocampal presynaptic terminals after acute stress. Cerebral Cortex, 28(3), 985-996. https://doi.org/10.1093/cercor/bhx008

Markovych, I. (2021). Neuroeconomics as a synthesis of economics, psychology and neurobiology.

McClure, S.M., Laibson, D.I., Loewenstein, G., & Cohen, J.D. (2004). Separate neural systems value immediate and delayed monetary rewards. Science, 306(5695), 503-507. https://doi.org/10.1126/science.1100907

Moody, G.D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly, 42(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853

Mrazek, M.D., Franklin, M.S., Phillips, D.T., Baird, B., & Schooler, J.W. (2013). Mindfulness training improves working memory capacity and GRE performance while reducing mind wandering. Psychological Science, 24(5), 776-781. https://doi.org/10.1177/0956797612459659

Mueller, S.T., Piper, B.J., Geerken, A.R., Dixon, K.L., Kroliczak, G., Olsen, R.K., & Alsip, C.L. (2010). Sensitivity and specificity of the Impulsive-Premeditated Aggression Scale (IPAS) for classifying impulsive and premeditated aggression. Personality and Individual Differences, 48(3), 279-284. https://doi.org/10.1016/j.paid.2009.10.014

Nurse, J.R., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. IEEE Security and Privacy Workshops, 214-228. https://doi.org/10.1109/SPW.2014.38

Nurse, J.R., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. IEEE Security and Privacy Workshops, IEEE, USA. https://doi.org/10.1109/SPW.2014.38

Preston, S.D., Buchanan, T.W., Stansfield, R.B., & Bechara, A. (2007). Effects of anticipatory stress on decision making in a gambling task. Behavioral Neuroscience, 121(2), 257-263. https://psycnet.apa.org/doi/10.1037/0735-7044.121.2.257

Proctor, R.W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Human factors, 57(5), 721-727. https://doi.org/10.1177/0018720815585906

Rao, R.P., Parigi, P., Glimcher, P., & Ryan, J. (2018). Biologically inspired strategies for defending against cyberattacks: Resource constraints, strategic reasoning and deception. Cognitive Research: Principles and Implications, 3(1), 1-29.

Riedl, R., & Javor, A. (2012). The biology of trust: Integrating evidence from genetics, endocrinology, and functional brain imaging. Journal of Neuroscience, Psychology, and Economics, 5(2), 63-91. https://psycnet.apa.org/doi/10.1037/a0026318

Serra, D. (2021). Decision-making: from neuroscience to neuroeconomics-an overview. Theory and Decision, 91(1), 1-80. https://doi.org/10.1007/s11238-021-09830-3

Takahashi, T. (2009). Theoretical frameworks for neuroeconomics of intertemporal choice. Journal of Neuroscience, Psychology, and Economics, 2(2), 75. https://psycnet.apa.org/doi/10.1037/a0015463

Tennison, M.N., & Moreno, J.D. (2012). Neuroscience, ethics, and national security: The state of the art. PLoS Biology, 10(3), e1001289. https://doi.org/10.1371/journal.pbio.1001289

Teper, R., Zhong, M., & Inzlicht, M. (2015). How emotions shape moral behavior: Some answers (and questions) for the field of moral psychology. Social and Personality Psychology Compass, 9(1), 1-14. https://doi.org/10.1111/spc3.12154

Thaler, R.H., & Sunstein, C.R. (2009). Nudge: Improving decisions about health, wealth, and happiness. Penguin.

Tom, S.M., Fox, C.R., Trepel, C., & Poldrack, R.A. (2007). The neural basis of loss aversion in decision-making under risk. Science, 315(5811), 515-518. https://doi.org/10.1126/science.1134239

Vance, A., Jenkins, J.L., Anderson, B., Bjornn, D.K., & Kirwan, C.B. (2020). Tuning out security warnings: Management Information Systems Research Center, University of Minnesota, MIS Quarterly, 44(2), 355-380.

Wittmann, B.C., Daw, N.D., Seymour, B., & Dolan, R.J. (2008). Striatal activity underlies novelty-based choice in humans. Neuron, 58(6), 967-973. https://doi.org/10.1016/j.neuron.2008.04.027

Yang, N., Singh, T., & Johnston, A. (2020). A replication study of user motivation in protecting information security using protection motivation theory and self-determination theory. AIS Transactions on Replication Research, 6(1), 10.

Yu, R. (2016). Stress potentiates decision biases: A stress induced deliberation-to-intuition (SIDI) model. Neurobiology of Stress, 3, 83-95. https://doi.org/10.1016/j.ynstr.2015.12.006

Does this article screen for similarity?

Yes

Conflict of Interest

The author have no conflicts of interest to declare. There is also no financial interest to report. The author certify that the submission is original work and is not under review at any other publication.

About the License

Cite this Article

Kritika, A Comprehensive Study on the Emerging Role of Neuroeconomics Dynamics in Cybersecurity, Asian Journal of Interdisciplinary Research, 7(2) (2024), 27-43. https://doi.org/10.54392/ajir2423