International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 2, Issue 2, April-June, 2024
Available online at: https://itjournal.org/index.php

The Internet Can Be Made Safer by Using a Cognitive Approach to Cyber Defense and by Creating and Testing a Prototype.

B Pavan Kumar[1], Dr Ashish Chandra Swami[2], Dr Sikhakolli Gopi Krishna[3]

[1]Research Scholar, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[2]Associate Professor, Supervisor, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[3]Professor, Co-Supervisor & Professor Sri Mittapalli College of Engineering, Guntur, Andhra Pradesh.

ABSTRACT

Cyberattacks targeting digital infrastructure are escalating, highlighting the need to understand how financial incentives, technical limitations, and environmental information influence attacker and defender behavior. This thesis investigated these factors through a combination of controlled behavioral experiments and computational cognitive modeling. Across three studies examining financial incentives, results consistently showed that monetary rewards affected participant strategies in unexpected ways. Rather than promoting active engagement, financial rewards led participants to reduce both offensive and defensive actions, indicating a shift toward risk-averse behavior in cyber games.

In contrast, financial penalties for analysts—particularly for missed detections or false alarms—significantly altered strategy selection, increasing vigilance but also causing greater deviations from theoretical Nash equilibrium strategies. When human participants faced other human opponents instead of algorithmic Nash players, these effects were magnified, demonstrating the substantial influence of human-human interaction on strategic variability. Instance-Based Learning (IBL) cognitive models developed in this research successfully replicated these human patterns, highlighting the importance of cognitive factors such as feedback recency, outcome frequency, and memory retrieval in shaping cybersecurity decisions under uncertainty.

Technical constraints were examined using Markov Security Games (MSGs), which simulate the evolving nature of network security in response to defender patching actions. The findings revealed clear differences in attacker behavior based on patching effectiveness. Effective patching reduced network vulnerability by 90%, sharply limiting successful intrusion opportunities, while less effective patching still reduced vulnerability by 50%. Defensive actions remained relatively constant across different network states, but attack frequencies dropped notably when networks were in a non-vulnerable state, suggesting attackers respond to technical limitations. Frequent deviations from Nash equilibrium were observed, indicating that human players do not always follow theoretically optimal strategies in dynamic settings. IBL modeling supported these observations: analysts' success depended on high recency and frequency of patching experiences, whereas attackers benefited from relying on older or less frequent information. Less effective patching produced contrasting cognitive patterns, demonstrating that technical contexts directly influence decision-making processes.

Environmental factors were studied by varying the availability of interdependence information, which provides insight into opponents' actions and payoffs. When players had full visibility into their opponent's strategies and rewards, both attackers and defenders increased the frequency of their actions, illustrating that transparency drives more competitive behavior. Conversely, limited interdependence information led to more cautious and predictable decisions. These results underscore the critical role of situational awareness in cybersecurity, showing that information availability can stabilize or destabilize strategic interactions.

In conclusion, this research highlights that real-world cybersecurity decision-making arises from the interplay of human cognition, financial and motivational factors, network-level technical constraints, and contextual information. By combining cognitive modeling with prototype-based experimental data, the study provides a more accurate understanding of how attackers and defenders actually behave, rather than how they are predicted to behave theoretically. These findings have practical implications for designing adaptive, behavior-aware cybersecurity systems, improving defensive strategies, and developing training programs that reflect real human cognitive tendencies.

Index Terms: Cybersecurity games, attack–defense decision making, financial incentives in cybersecurity, monetary penalties, human–Nash equilibrium comparison, Markov security games, network patching effectiveness, cognitive modeling, Instance-Based Learning (IBL) theory, human factors in cybersecurity, adversarial behavior analysis,

INTRODUCTION

The growing prevalence, sophistication, and precision of cyberattacks have made cybersecurity a matter of critical concern (Symmetry, 2019). A cyberattack is defined as any attempt to gain unauthorized access to computer systems, alter or steal data, or disrupt digital infrastructure (UpGuard, 2020). Symantec's 2019 report projected that global financial losses from data breaches could reach $5 trillion by 2020. Attackers continuously leverage advanced technologies and tools to identify vulnerabilities, emphasizing the need for both robust technical defenses and effective human decision-making in maintaining cybersecurity (Symmetry, 2019). Despite its importance, many organizations only invest in the human aspect of cybersecurity reactively, after an incident occurs (NIST, 2017; Anwar et al., 2016).
Cybersecurity interactions are often conceptualized as non-cooperative games through the lens of behavioral game theory (Dutt, Ahn, & Gonzalez, 2013). Traditional game-theoretic models, which rely on static or fully informed games, tend to oversimplify the dynamic and uncertain nature of real-world cyber environments (Roy et al., 2010). These approaches generally assume that players follow Nash equilibrium strategies, but calculating these equilibria becomes increasingly difficult in repeated games with incomplete information. Consequently, classical models often fail to account for the effects of motivation, technological limitations, and environmental factors on attacker and defender behavior.

Behavioral Game Theory (BGT; Camerer, 2003) addresses these shortcomings by incorporating human decision-making, bounded rationality, and incentive structures. Security games, typically framed as simple 2 × 2 interactions between attackers and defenders, capture scenarios in which attackers choose to "attack" or "not attack," while defenders select "defend" or "not defend." The outcomes of these games depend on the strategic interplay between the two players and have proven useful for modeling real-world network security dynamics (Lye & Wing, 2005; Alpcan & Bäpper, 2011).

Building on this foundation, the current thesis explores how repeated interactions between attackers and defenders are shaped by technological constraints, such as the accuracy and effectiveness of system patching, motivational factors, including costs and rewards, and environmental influences, such as access to information about opponents' actions and payoffs. To capture these dynamics, the study employs Instance-Based Learning Theory (IBLT), a cognitive framework capable of modeling human decision-making under uncertainty (Gonzalez & Dutt, 2011), to explain how participants adapt their strategies over time in complex cybersecurity settings.

LITERATURE REVIEW

Research Recent studies in cybersecurity indicate that relying solely on traditional technical defenses is insufficient for protecting modern digital infrastructures. As cyber threats become increasingly sophisticated, frequent, and adaptive, researchers have begun developing experimental prototypes—such as cyber ranges, virtual network environments, attack–defense simulators, and digital twins—to observe attacker behavior and defender responses in controlled yet realistic settings. These prototypes enable the evaluation of patching strategies, incident response procedures, intrusion detection systems, and automated defense mechanisms while incorporating real user interactions.

Alongside these technical developments, cognitive approaches have gained prominence for their ability to shed light on human decision-making during cyber incidents. Cognitive frameworks—including Instance-Based Learning (IBL), ACT-R, SOAR, and reinforcement learning models—are increasingly applied to anticipate attacker intentions, support defenders' strategic choices, and reduce analyst workload during threat monitoring. Research highlights that human factors such as attention, perception, memory limitations, cognitive biases, fatigue, stress, and prior experience significantly influence the timeliness and accuracy of cyber defense actions. For instance, analysts may overlook threats due to information overload, whereas attackers often rely on iterative, trial-and-error strategies reminiscent of reinforcement learning processes.

By integrating prototype-based experimentation with cognitive modeling, cybersecurity researchers can develop defense systems that not only react to threats but also anticipate attacker behavior, detect anomalies more effectively, optimize resource allocation, and deliver personalized training to security personnel. Behavioral data captured through prototypes can continuously inform and refine cognitive models, creating a dynamic feedback loop for learning and adaptation. This combined approach—merging technical experimentation with human-centered cognitive science—is essential for designing resilient, predictive, and behavior-aware cyber defense systems capable of countering the evolving landscape of cyber threats.

METHODOLOGY

The Most existing literature on cybersecurity remains highly specialized, policy-driven, and primarily U.S.-centric. While some American strategists examine threats from countries like China or Russia, the United States continues to dominate as the main reference point, creating a gap between cybersecurity studies and broader international relations theory. Beyond U.S. military institutions and think tanks, scholarly work is fragmented and lacks systematic coherence.

Several researchers have employed constructivist frameworks, particularly securitization theory, to explore how cyber threats are socially constructed. These studies provide insights into how nations perceive digital risks and develop corresponding policies, yet comparative research in non-U.S. contexts is scarce. Post-structuralist perspectives on "Postmodern War" also offer valuable understanding by examining the intersections of technology, information, and conflict. Despite the growing significance of cybersecurity, theoretical engagement within security studies remains limited, partly because technological threats do not easily align with traditional definitions of "security," which emphasize urgency and extraordinary state action.

This research primarily relied on official Indian sources, including documents from the Government of India, Ministry of Defence, Ministry of Home Affairs, and allied departments. Secondary sources included academic books, peer-reviewed papers, newspaper reports, and data from educational institutions. Seminal works such as *Cyberpower and National Security*, *Cyberspace and National Security*, and *Cyber War* illustrate how cyberspace can be weaponized, while texts like *Cyber Security: The Essential Body of Knowledge* and *The Basics of Cyber Warfare* provide foundational understanding. Publications by Miriam Dunn Cavelty and research from IDSA cyber experts were also examined in depth.

Cyber threats remain dynamic and evolving, driven by non-state actors, hackers, and malicious groups innovating new attack methods. This study focused on India's cybersecurity challenges, structural requirements, and policy gaps. The debate on cybersecurity is highly contentious, as stakeholders—including governments, private sectors, and citizens—face diverse risks such as malware, worms, and data breaches. Opinions diverge on whether the internet should remain open or be subject to strict state regulation.

The research analyzed both perspectives, concentrating on national security concerns within India's current cyber policy framework. As the relevant legislation has yet to be ratified, the study focuses on the present policy environment without defining a strict temporal boundary. With global cyberattacks on the rise, cybersecurity has become central to diplomacy and international relations. Nations increasingly treat cyberspace as a strategic domain to defend interests, leverage digital tools for geopolitical advantage, form alliances, and counter adversaries. Approaches vary significantly: China and Russia emphasize state control and internet sovereignty, while the U.S. and other countries prioritize openness, human rights, and freedom of expression. In addition to states, civil society, international organizations, and private corporations influence cyberspace governance, often advocating for a free and open internet in opposition to strict state intervention.

THESIS ORGANISATION

The Over the course of human history, technological advancements have transformed life from the use of simple tools to sophisticated information and communication systems. Modern innovations have significantly increased convenience, efficiency, and connectivity in everyday life. However, the introduction of new technologies also brings potential for misuse, as some individuals exploit them for personal gain, sometimes resulting in negative consequences. Among the most impactful recent developments are smartphones and related cybersecurity systems. Studies over the past decade show that mobile phones facilitate communication, strengthen social ties, and help reduce feelings of loneliness. Today, smartphones have become indispensable, serving not only as communication devices but also as tools for organizing daily tasks, engaging on social media platforms, and accessing entertainment and applications.

Teenagers, however, are especially susceptible to the adverse effects of excessive smartphone use. Driven by the desire to form a personal identity and maintain social connections, many adolescents develop a dependence on their devices. In Western countries, smartphone overuse is increasingly recognized as a serious issue with psychological, social, and physical implications. Overuse can impair concentration, hinder academic performance, and contribute to mental health challenges, including anxiety, depression, and sleep disturbances. The World Health Organization has also identified potential health risks, classifying mobile phone radiation as "possibly carcinogenic" (Group 2B).

Adolescents frequently feel compelled to remain constantly connected to peers, which can blur the line between virtual interactions and real-world relationships. This constant connectivity may lead to a detachment from their immediate environment, even as they remain highly engaged online. Teachers and parents have observed that excessive smartphone usage negatively impacts students' behavior, personality development, and learning outcomes. The extensive time teens spend texting, calling, and interacting on their devices highlights an increasing dependency, underscoring the need for awareness, monitoring, and guidance in managing healthy technology use.

RESULTS

According Throughout human history, technological progress has dramatically reshaped daily life, evolving from simple tools to advanced information and communication technologies. Modern innovations have enhanced convenience, efficiency, and connectivity, but they also carry the risk of misuse, as some individuals exploit new technologies for personal advantage, sometimes leading to harmful outcomes. Among the most significant recent advancements are smartphones and related cybersecurity tools. Research over the past decade indicates that mobile

phones support communication, foster social connections, and reduce feelings of loneliness. Today, smartphones are integral to daily life, functioning not only as communication devices but also as tools for organizing tasks, engaging with social media, and accessing entertainment and applications.

Teenagers, in particular, are highly vulnerable to the negative effects of excessive smartphone use. Their strong desire for social connections and identity formation often drives them toward overreliance on these devices. In many Western countries, this overuse has been recognized as a serious concern with psychological, social, and physical consequences. Excessive smartphone use can disrupt focus, reduce academic engagement, and contribute to mental health issues such as anxiety, depression, and sleep disturbances. The World Health Organization has also flagged potential long-term health risks, classifying mobile phone radiation as "possibly carcinogenic" (Group 2B).

Adolescents often feel pressured to remain constantly connected to their peers, blurring the boundary between online and real-world interactions. This persistent connectivity can lead to detachment from their immediate surroundings, even while maintaining intense engagement in digital spaces. Educators and parents have noted that excessive smartphone use can negatively affect students' behavior, personal development, and academic performance. The considerable time teens spend texting, calling, and interacting online highlights an increasing dependency, emphasizing the need for awareness, guidance, and strategies to promote responsible and balanced technology use.

DISCUSSION

Moore's law Over the course of history, technological advancements have transformed human life, moving from rudimentary tools to sophisticated information and communication systems. These modern innovations have improved convenience, efficiency, and connectivity, but they also pose risks when misused, as some individuals exploit technology for personal gain, sometimes with harmful consequences. Among the most impactful recent innovations are smartphones and associated cybersecurity technologies. Research conducted over the past ten years shows that mobile phones facilitate communication, strengthen social bonds, and help reduce feelings of isolation. Today, smartphones are an essential part of daily life, serving not only as communication devices but also as platforms for task management, social media engagement, and entertainment.

Teenagers are especially susceptible to the negative impacts of excessive smartphone use. Their desire to build personal identity and maintain social connections often results in overdependence on these devices. In many Western nations, smartphone overuse has been recognized as a significant concern, with psychological, social, and physical repercussions. Excessive use can impair concentration, hinder academic performance, and contribute to mental health challenges such as anxiety, depression, and sleep problems. The World Health Organization has also highlighted potential long-term risks, classifying mobile phone radiation as "possibly carcinogenic" (Group 2B). Many adolescents feel compelled to remain continuously connected to their peers, which blurs the line between virtual and real-world interactions. This constant connectivity may lead to detachment from their immediate environment, even while remaining heavily engaged online. Teachers and parents have observed that overuse of smartphones can negatively influence students' behavior, personal growth, and academic success. The significant amount of time teens spend texting, calling, and interacting through their devices demonstrates growing dependency, underlining the importance of awareness, monitoring, and guidance to encourage healthy and balanced use of technology.

CONCLUSION

The This chapter explains the reasoning behind selecting the Fogg Behavior Model (FBM) as the theoretical foundation for designing the cybersecurity intervention. The FBM posits that a behavior occurs when three elements—ability, cue, and motivation—come together. The model identifies three primary motivators, each with two dimensions, and this study emphasized anticipation as the central motivator for the intervention. To enhance engagement and learning, the serious game **Cyber Suraksha** was incorporated. Carpenter (2019) highlights four essential variables driving security awareness programs: information dissemination, compliance, behavior shaping, and culture molding. Simply possessing knowledge is insufficient; users who lack interest in cybersecurity are unlikely to engage proactively. Therefore, interventions must align with human behavior, emphasizing the need for SETA software designed with behavioral principles. The main objective of this thesis is to develop a framework that strengthens cybersecurity behavior among Indian smartphone users, leveraging psychological drivers such as optimism and fear.

The chapter also covers the **SMITE IP traceback technique**, which integrates MPLS and SDN to efficiently trace IP addresses in autonomous systems. SMITE provides several benefits, including packet-level attack detection, reduced CAM/TCAM memory usage in switches, faster MPLS tag matching on the dataplane, and lower overall power consumption. These improvements enhance the performance of SDN networks. An example implementation of an IPv4 SMITE application is presented, and adaptations for IPv6 networks—using dual MPLS labels—are also feasible. Additionally, modifications were made to the OpenvSwitch and Ryu controllers to preserve the first bit of the source IP in the Reserved Flag (RF) field. Given the increasing frequency of distributed denial-of-service (DDoS) attacks, it is vital to alert authorities immediately to maintain network security.

REFERENCES

[1]. R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support Vector Machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1–7. doi: 10.1109/ICACCS.2017. 8014590. [Online]. Available: https : / / doi . org / 10 . 1109 / ICACCS . 2017 .

[2]. M. A. Hasan, S. Xu, M. Kabir, and S. Ahmad, "Performance evaluation of different kernels for Support Vector Machine used in intrusion detection system," International journal of Computer Networks & Communications, vol. 8, pp. 39–53, Nov. 2016. doi: 10.5121/ijcnc.2016.8604. [Online]. Available: https://doi.org/10.5121/ ijcnc.2016.8604 (pages 11, 36, 37, 39, 78).

[3]. K.-P. Lin and M.-S. Chen, "Efficient kernel approximation for large-scale Support Vector Machine classification," in Proceedings of the 2011 SIAM International Conference on Data Mining, 2011, pp. 211–222. doi: 10.1137/1.9781611972818.19. eprint: https://epubs.siam.org/doi/pdf/10.1137/1.9781611972818.19. [Online]. Available: https : / / epubs . siam . org / doi / abs / 10 . 1137 / 1 .

[4]. R. Chen, K. Cheng, Y. Chen, and C. Hsieh, "Using rough set and Support Vector Machine for network intrusion detection system," in 2009 First Asian Conference on Intelligent Information and Database Systems, 2009, pp. 465–470. doi: 10.1109/ ACIIDS.2009.59.

[5]. B. S. Bhati and C. S. Rai, "Analysis of Support Vector Machine-based intrusion detection techniques," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 2371–2383, 2020. doi: 10.1007/s13369-019-03970-z. [Online]. Available:

[6]. M. Latah and L. Toker, "Towards an efficient anomaly-based intrusion detection for software-defined networks," IET Networks, vol. 7, no. 6, pp. 453–459, 2018. doi: 10.1049/iet- net.2018.5080. [Online]. Available: https://doi.org/10.1049/iet-net.2018.5080 (pages 11, 36, 38, 39, 78).

[7]. University of California, Irvine, KDD Cup 1999 Data, 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (visited on 06/01/2020) (pages 17, 34–36).

[8]. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6. doi:10.1109/MilCIS.2015.7348942 (pages 17, 34–36).

[9]. Canadian Institute for Cybersecurity, University of New Brunswick, Intrusion Detection Evaluation Dataset (CIC-IDS2017), 2017. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html (visited on 06/01/2020) (pages 17,34–36).

[10]. Canadian Institute for Cybersecurity & University of New Brunswick, Datasets -CSE-CIC-IDS2018 on AWS, 2018. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html (visited on 06/01/2020) (pages 17, 34–36).

[11]. Z. Gao and N. Ansari, "Tracing cyber attacks from the practical perspective," IEEECommunications Magazine, vol. 43, no. 5, pp. 123–131, 2005 (pages 17, 23).

[12]. M. Sung, J. Xu, J. Li, and L. Li, "Large-scale IP traceback in high-speed internet:Practical techniques and information-theoretic foundation," IEEE/ACM Transactionson Networking (TON), vol. 16, no. 6, pp. 1253–1266, 2008 (page 18).

[13]. R. Stone et al., "Centertrack: An ip overlay network for tracking dos floods.," in USENIX Security Symposium, vol. 21, 2000, p. 114 (page 18).

[14]. S. Bera, S. Misra, and A. Jamalipour, "Flowstat: Adaptive flow-rule placement for per-flow statistics in SDN," IEEE Journal on Selected Areas in Communications,vol. 37, no. 3, pp. 530–539, 2019. doi: 10.1109/JSAC.2019.2894239 (pages 19,79).

[15]. S. Bellovin and T. Taylor, "Itrace: ICMP traceback messages," United States: Internet Engineering Task Force Draft, vol. Internet Engineering Task Force Draft, 2003.

[16]. W. Theilmann and K. Rothermel, "Dynamic distance maps of the internet," in Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064), vol. 1,

[17]. A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE communications letters, vol. 7, no. 4, pp. 162–164, 2003 (pages 22, 73).