

Nonlinear Threats and Adaptive Defenses: A Complexity Perspective on Cybersecurity Challenges

DOI: 10.5281/zenodo.15575481

Jan Mark S. Garcia, MIT, DIT-CAR

West Visayas State University-Himamaylan City Campus,
Himamaylan City, Negros Occidental, Negros Island, Philippines
<https://orcid.org/0000-0002-3306-0507> | markjj06.garcia@wvsu.edu.ph

Abstract

The dynamic and rapidly evolving nature of cyber threats has rendered traditional, static security models increasingly obsolete. This study investigates the role of complexity science in understanding and mitigating nonlinear cybersecurity threats, characterized by unpredictable, emergent behaviors and systemic impact. By integrating an in-depth literature review with simulation-based experimentation, the research evaluates the performance of adaptive defense systems modeled on the principles of complex adaptive systems (CAS). Findings indicate substantial improvements over traditional models, including an 88% reduction in detection time, a 76% decrease in false positives, and enhanced system resilience under multi-vector and zero-day attack scenarios. These results validate the hypothesis that complexity-informed architectures significantly enhance cyber resilience. The study's novelty lies in its empirical demonstration of how self-organizing, feedback-driven systems can serve as a scalable framework for next-generation cybersecurity. It contributes to both theoretical advancement and practical application, offering policymakers and security architects a scientific foundation for designing proactive, anticipatory defense mechanisms in an increasingly hostile digital environment. The study also discusses limitations and suggests directions for future research, including real-world deployment challenges and ethical considerations.

Keywords: Cybersecurity, Complexity Science, Adaptive Defense, Nonlinear Threats, Cyber Resilience, Simulation

Introduction

Background

The cyber threat landscape has undergone a profound transformation, evolving into a highly interconnected and dynamic ecosystem where traditional, static security models are increasingly inadequate. Conventional cybersecurity tools, which rely heavily on fixed rules, signatures, and reactive paradigms, are ill-equipped to counter sophisticated and evolving threats such as advanced persistent threats (APTs), zero-day vulnerabilities, polymorphic malware, and multi-stage attack campaigns (Zhou and Tang, 2020). Landmark cyberattacks including the SolarWinds supply chain compromise in 2020, the Colonial Pipeline ransomware incident in 2021, the Microsoft Exchange server breach in 2021, and the MOVEit Transfer vulnerability exploitation in 2023 vividly illustrate the growing complexity, unpredictability, and systemic impact of modern cyber threats (Salman and Habib, 2022; Tavabi and Geer, 2023). These threats are inherently nonlinear and emergent, manifesting behaviors that cannot be predicted solely through analysis of individual components but rather arise from complex interactions among attackers, defenders, and the digital infrastructure itself. The highly interconnected nature of contemporary IT environments means that local security failures can cascade into widespread operational disruptions, amplifying their impact (Alevizos, 2025). Consequently, cybersecurity requires a shift from static, centralized defenses toward more dynamic, distributed, and adaptive systems capable of learning and evolving alongside threats.

Complexity science, an interdisciplinary field focused on understanding systems composed of numerous interacting agents exhibiting nonlinear dynamics and emergent behaviors, provides valuable theoretical and practical tools for addressing these challenges (Salman and Habib, 2022). Core concepts such as emergence, self-organization, feedback loops, and adaptability underpin complex adaptive systems (CAS), which have proven effective in diverse domains ranging from ecology to economics (Ahmadi, 2025). Applying these principles to cybersecurity suggests a new paradigm where defense mechanisms autonomously organize, adapt, and anticipate threats, much like biological immune systems that continuously evolve to detect and neutralize novel pathogens (Tavabi and Geer, 2023). CAS-based cybersecurity architectures leverage machine learning, reinforcement learning, and agent-based modeling to facilitate decentralized, continuous learning and response capabilities (Alshamrani and Alshahrani, 2023; Huang et al., 2021). These adaptive systems have the potential to dramatically reduce detection times, minimize false positives, and enhance resilience against zero-day exploits and multi-vector attacks, thereby offering a scalable solution to the complexities of the modern threat environment (Mofijul and Nasser, 2024).

Research Problem

Current cybersecurity models predominantly operate reactively with limited adaptability, leading to delayed detection

and ineffective responses. While machine learning techniques have improved detection rates, they are often siloed and lack integration within a systemic, complexity-informed framework. This gap restricts scalability, adaptability, and robustness in real-world deployments against nonlinear, emergent threats.

Objectives

1. Define nonlinear cyber threats within a complexity science framework
2. Evaluate limitations of static cybersecurity models
3. Experimentally assess adaptive defense systems inspired by complex adaptive systems (CAS)
4. Propose a scalable framework for complexity-based cybersecurity architecture

Literature Review

The rapidly evolving cyber threat landscape necessitates a shift from static, reactive security models to dynamic and adaptive defense mechanisms. Traditional cybersecurity approaches, heavily reliant on fixed rules and signatures, are proving increasingly inadequate against sophisticated and nonlinear threats such as advanced persistent threats (APTs), zero-day vulnerabilities, polymorphic malware, and multi-stage attack campaigns. Recent landmark cyberattacks, including the SolarWinds supply chain compromise (2020), the Colonial Pipeline ransomware incident (2021), the Microsoft Exchange server breach (2021), and the MOVEit Transfer vulnerability exploitation (2023), vividly demonstrate the growing complexity, unpredictability, and systemic impact of modern cyber threats. These threats are inherently nonlinear and emergent, with behaviors arising from complex interactions among attackers, defenders, and the digital infrastructure itself.

Limitations of Traditional Cybersecurity Models

Conventional cybersecurity tools suffer from significant limitations when confronted with the dynamic nature of contemporary cyber threats. They operate predominantly reactively, leading to delayed detection and ineffective responses. Their reliance on static signatures and rule-based heuristics makes them vulnerable to dynamic, polymorphic, and multi-vector attacks. This lack of flexibility, systemic awareness, and resilience often results in delayed detection and an excessive number of false alarms. Furthermore, centralized architectures, common in traditional models, fail to effectively capture cascading failures and emergent behaviors that characterize modern cyberattacks. While machine learning techniques have contributed to improved detection rates, they often function in silos, lacking integration within a broader systemic, complexity-informed framework, which restricts their scalability, adaptability, and robustness in real-world deployments.

The Promise of Complexity Science and Adaptive Defense Systems

Complexity science, an interdisciplinary field focused on understanding systems with numerous interacting agents exhibiting nonlinear dynamics and emergent behaviors, offers valuable theoretical and practical tools for addressing these challenges. Core concepts such as emergence, self-organization, feedback loops, and adaptability are central to complex adaptive systems (CAS). The application of these principles to cybersecurity suggests a new paradigm where defense mechanisms autonomously organize, adapt, and anticipate threats, much like biological immune systems continuously evolve to detect and neutralize novel pathogens.

Several studies and theoretical works underscore the potential of adaptive, complexity-informed cybersecurity architectures:

1. **Reinforcement Learning and Agent-Based Modeling:** CAS-based cybersecurity architectures leverage advanced techniques such as machine learning, reinforcement learning, and agent-based modeling to facilitate decentralized, continuous learning and response capabilities. Alshamrani and Alshahrani (2023) have explored adaptive cyber defense techniques based on multiagent reinforcement learning strategies, contributing to improved system responses. Similarly, Huang and Zhu (2021) have investigated combating informational denial-of-service (IDoS) attacks through modeling and mitigation of attentional human vulnerability, further demonstrating the utility of adaptive learning approaches. Ahmadi (2025) discusses adaptive cybersecurity, specifically focusing on dynamically retrainable firewalls for real-time network protection, indicating a move towards more agile defensive postures.
2. **Enhanced Resilience and Self-Organization:** These adaptive systems have the potential to dramatically reduce detection times, minimize false positives, and enhance resilience against zero-day exploits and multi-vector attacks, offering a scalable solution to the complexities of the modern threat environment. The principles of complex adaptive systems enable emergent properties such as autonomous network segmentation and robust redundancy, significantly enhancing overall cyber resilience. Alevizos (2025) also proposes a complexity-informed approach to optimize cyber defenses, reinforcing the theoretical foundation for such systems.

3. **Biological Immune System Analogy:** The analogy to the biological immune system is particularly instructive, as its decentralized, adaptive detection and response mechanisms provide a model for rapid neutralization of novel threats in cybersecurity. This concept resonates with the idea of a continuously evolving defense mechanism.

Identified Research Gaps

Despite the growing recognition of complexity science and the individual advancements in machine learning techniques for cybersecurity, significant research gaps persist, which this study aims to address:

1. **Lack of Systemic, Complexity-Informed Frameworks:** Current cybersecurity models, while incorporating some advanced techniques, predominantly operate reactively with limited adaptability. A key gap is the lack of integration of these techniques within a systemic, complexity-informed framework that can fully leverage the principles of CAS.
2. **Scalability and Robustness in Real-World Deployments:** The absence of such a comprehensive framework restricts the scalability, adaptability, and overall robustness of defense mechanisms in real-world deployments, particularly against nonlinear and emergent threats.
3. **Empirical Validation of Adaptive Systems:** While theoretical arguments for adaptive systems exist, there is a need for empirical demonstration and evaluation of their performance against traditional models under controlled, yet realistic, simulation environments. This study aims to fill this gap by experimentally assessing adaptive defense systems inspired by CAS.
4. **Developing a Scalable Framework:** The current literature often highlights components of adaptive defense but lacks a clear, scalable framework for implementing complexity-based cybersecurity architecture that integrates self-organizing and feedback-driven systems effectively.

This study's novelty lies in its empirical demonstration of how self-organizing, feedback-driven systems can serve as a scalable framework for next-generation cybersecurity. By integrating an in-depth literature review with simulation-based experimentation, the research evaluates the performance of adaptive defense systems modeled on CAS principles, directly addressing the limitations of static models and the need for more resilient and anticipatory defense mechanisms.

Methodology

Research Design

This study adopts a mixed-methods approach, combining qualitative case study analysis with quantitative simulation experiments to evaluate and compare traditional and adaptive cybersecurity models. The mixed-methods approach was chosen to enable triangulation of results, enhancing validity and providing both empirical performance data and contextual understanding of nonlinear threat behaviors.

Data Collection

1. **Literature Review:** A comprehensive review of 48 peer-reviewed articles published between 2020 and 2025 was conducted to identify and synthesize relevant complexity science concepts applicable to cybersecurity. The literature spans interdisciplinary domains including computer science, complexity theory, systems engineering, and cybersecurity.
2. **Case Studies:** Ten significant cyber incidents, including SolarWinds, Microsoft Exchange vulnerabilities, Colonial Pipeline ransomware attack, and MOVEit data breach, were examined to uncover nonlinear characteristics, multi-vector attacks, and cascading systemic impacts. Data was extracted from publicly available incident reports, government advisories, and academic analyses, and thematically coded to identify emergent threat patterns.
3. **Simulations:** Synthetic datasets replicating sophisticated attack vectors such as Distributed Denial of Service (DDoS) attacks, zero-day exploits, and lateral movements were generated using open-source platforms CybORG, MITRE Caldera, and DeterLab. Two cybersecurity defense models were evaluated under identical attack scenarios: a traditional fixed-rule model and an adaptive CAS-based model. Metrics measured included detection speed, false positive rates, response latency, and mitigation effectiveness.

Data Analysis

1. **Qualitative Analysis:** Thematic coding and content analysis were used to identify recurring nonlinear threat behaviors and adaptive defense patterns in the case studies.
2. **Quantitative Analysis:** Statistical tests (t-tests and ANOVA) were performed using Python and R to compare the detection times, false positive rates, response latencies, and mitigation success rates between

traditional and adaptive models. Confidence intervals and effect sizes were reported to demonstrate statistical and practical significance.

Results

Characteristics of Nonlinear Cyber Threats

- Analysis confirmed that nonlinear cyber threats exhibit:
1. Emergence: Threat behaviors arise unpredictably through complex attacker-defender interactions.
 2. Adaptability: Attack vectors mutate dynamically, evading static detection mechanisms.
 3. Systemic Impact: Compromises cascade through interconnected networks, amplifying damage.

Case Study	Multi-Vector Attack	Adaptive Behavior	Systemic Impact
SolarWinds	Yes	Yes	High
Colonial Pipeline	Yes	Partial	High
Microsoft Exchange	Yes	Yes	Medium
MOVEit Transfer	Yes	Yes	High

Simulation Performance Comparison

Metric	Traditional Model	Adaptive Model
Detection Time	2.3 hours	17 minutes
False Positive Rate	21 percent	5 percent
Response Latency	45 minutes	10 minutes
Mitigation Success	69 percent	93 percent

The adaptive system, built on reinforcement learning and agent-based modeling, demonstrated superior performance through self-tuning, emergent network segmentation, and robust redundancy.

Detailed Simulation Setup

Component	Description	Tools/Parameters Used
Attack Types	DDoS, zero-day exploits, lateral movement, multi-vector campaigns	CybORG scenarios, MITRE Caldera framework
Simulated Dataset Generation	Synthetic network traffic, system calls, alerts with injected attacks	DeterLab, synthetic trace generators
Defense Models Compared	1. Traditional fixed-rule IDS	

Component	Description	Details/Tools Used
Defense Model	Adaptive CAS-inspired RL agent-based model	Signature databases vs. reinforcement learning agents
Metrics Measured	Detection time, false positives, response latency, mitigation success	Automated metric logging via simulation tools
Environment	Simulated enterprise network with diverse nodes	500 nodes, mixed OS (Windows/Linux), CybORG network topology
Simulation Duration	Time span for each simulation run	48 simulated hours per run
Repetitions	Number of times each scenario was run for statistical significance	30 runs per scenario, randomized attack pattern seeds

Statistical Analysis Summary

Metric	Traditional Model Mean	Adaptive Model Mean	P-Value	Effect Size (Cohen's d)	Interpretation
Detection Time (min)	138	17	<0.001	2.3	Large significant improvement
False Positive Rate (%)	21	5	<0.001	1.8	Large significant reduction

RESPONSE LATENCY (MIN)	45	10	<0.001	1.9	Large significant improvement
MITIGATION SUCCESS (%)	69	93	<0.001	2.1	Large significant improvement

Two-tailed t-tests confirmed all differences were highly statistically significant.

Discussion

Limitations of Traditional Cybersecurity Models

Traditional cybersecurity defenses rely heavily on static signatures and rule-based heuristics, becoming ineffective against dynamic, polymorphic, and multi-vector threats (Zhou and Tang, 2020). These models lack flexibility, systemic awareness, and resilience, causing delayed detection and excessive false alarms (Karegar et al., 2022). Centralized architectures also fail to capture cascading failures and emergent behaviors (Salman and Habib, 2022).

Complexity Science as a Transformative Framework

Complex adaptive systems (CAS) principles provide a pathway to overcome these limitations. Adaptive cybersecurity architectures with self-organization, distributed sensing, and continuous learning enable proactive, real-time responses (Ahmadi, 2025). Reinforcement learning and agent-based approaches dynamically evolve defenses, improving accuracy and reducing false positives (Alshamrani and Alshahrani, 2023; Huang et al., 2021). Emergent properties such as autonomous network segmentation and redundancy enhance resilience (Mofijul and Nasser, 2024). The biological immune system analogy is instructive: decentralized, adaptive detection and response enable rapid neutralization of novel pathogens, a principle cybersecurity can emulate for robustness and agility (Tavabi and Geer, 2023).

Limitations of This Study

While simulations provide valuable insights, the study's findings are limited by the synthetic nature of datasets and the controlled environment, which may not fully capture real-world complexity or adversary ingenuity. The adaptive models require significant computational resources, which may pose deployment challenges in resource-constrained environments. Further, ethical and privacy implications of autonomous defense mechanisms need comprehensive examination before practical application.

Ethics and Policy Considerations

Adaptive cybersecurity systems, while promising, raise critical ethical and policy issues:

1. **Autonomy versus Control:** Autonomous adaptive defense systems must incorporate human oversight to prevent unintended or harmful automated responses.
2. **Privacy:** Continuous monitoring required by adaptive systems poses privacy risks, necessitating strict compliance with data protection laws such as GDPR and HIPAA, and adherence to privacy-by-design principles.
3. **Bias and Fairness:** Machine learning models may inherit biases from training data, potentially causing unfair treatment or missing certain threats. Transparent algorithms and regular audits are essential.
4. **Accountability:** Clear frameworks must be established to assign responsibility when autonomous defenses cause unintended damage or fail.

Policy Recommendations:

1. Establish international standards for complexity-based adaptive cybersecurity architectures.
2. Mandate transparency and explainability for machine learning-driven defense mechanisms.
3. Require regular ethical reviews and compliance audits during system deployment and operation.
4. Promote interdisciplinary research integrating complexity science, cybersecurity, ethics, and human factors.

Implications for Policy, Research, and Practice

Complexity-informed cybersecurity frameworks must be integrated into standards such as NIST and ISO (NIST, 2021). Funding should prioritize interdisciplinary research at the intersection of complexity science, machine learning, and cybersecurity (Alevizos, 2025; Karegar et al., 2022). Organizations need to transition from reactive to anticipatory defense postures, adopting complexity metrics and adaptive architectures to enhance resilience.

Future Work

Future research should focus on validating adaptive CAS-based models in real-world operational environments,

addressing scalability, interoperability, and user trust issues. Developing transparent, explainable adaptive defense mechanisms and incorporating human factors will be critical for widespread adoption. Ethical frameworks guiding autonomous cybersecurity responses must be established to mitigate risks of unintended consequences.

Conclusion

This research highlights the critical role of complexity science in advancing cybersecurity architectures to address nonlinear threats. The empirical evidence confirms that adaptive, self-organizing defense systems outperform traditional static models, offering a scalable, resilient framework for future cyber defense. By embracing complexity-informed design principles, cybersecurity can evolve from reactive patches to proactive, dynamic protection, safeguarding digital infrastructures in an increasingly hostile and uncertain threat landscape.

References

- Acuto, A., & Maskell, S. (2023). Entity-based reinforcement learning for autonomous cyber defence. In *Proceedings of the Workshop on Autonomous Cybersecurity* (pp. 1–6). ACM. <https://doi.org/10.1145/3689933.3690835>
- Adams, M. D., Hitefield, S. D., Hoy, B., Fowler, M. C., & Clancy, T. C. (2013). Application of cybernetics and control theory for a new paradigm in cybersecurity. *arXiv preprint*. <https://arxiv.org/abs/1311.0257>
- Aggarwal, R., & Aggarwal, R. (2024). Dynamic awareness and strategic adaptation in cybersecurity: A game-theory approach. *Games*, 15(2), 13. <https://doi.org/10.3390/g1502013>
- Ahmadi, S. (2025). Adaptive cybersecurity: Dynamically retrainable firewalls for real-time network protection. *arXiv preprint*. <https://arxiv.org/abs/2501.09033>
- Alevizos, L. (2025). A complexity-informed approach to optimise cyber defences. *arXiv preprint*. <https://arxiv.org/abs/2501.15578>
- Alshamrani, A., & Alshahrani, A. (2023). Adaptive cyber defense technique based on multiagent reinforcement learning strategies. *Intelligent Automation & Soft Computing*, 36(3), 2757–2771. <https://doi.org/10.32604/iasc.2023.032835>
- Chen, H., Cam, H., & Xu, S. (2021). Quantifying cybersecurity effectiveness of dynamic network diversity. *arXiv preprint*. <https://arxiv.org/abs/2112.07826>
- Colarik, A., & Janczewski, L. (2015). Establishing cyber warfare doctrine. In *Current and Emerging Trends in Cyber Operations* (pp. 37–50). Palgrave Macmillan.
- Collier, S. J., & Lakoff, A. (2008). Distributed preparedness: The spatial logic of domestic security in the United States. *Environment and Planning D: Society and Space*, 26, 7–28.
- Collier, S. J., & Lakoff, A. (2008). The vulnerability of vital systems: How 'critical infrastructure' became a security problem. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *The politics of 'securing the homeland': Critical infrastructure, risk, and (in)security* (pp. 17–39). Routledge.
- Collier, S. J., & Lakoff, A. (2014). Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture & Society*. <https://doi.org/10.1177/0263276413510050>
- Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4, 15–32.
- Dillon, M. (2002). Network society, network-centric warfare and the state of emergency. *Theory, Culture & Society*, 19(4), 71–79.
- Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2016). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. Apress.
- Douglas, M., & Wildavsky, A. B. (1983). *Risk and culture: An essay on the selection of technical and environmental dangers*. University of California Press.
- Enderle, R. (2021). *Cybersecurity: The essential body of knowledge*. Springer.
- Ferrell, O. C., Fraedrich, J., & Ferrell, L. (2023). *Business ethics: Ethical decision making & cases*. Cengage Learning.
- Flynn, S. E. (2015). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Galinec, D., & Macanga, D. (2012). Observe, orient, decide and act cycle and pattern-based strategy: Characteristics and complementation. In *Proceedings of the Central European Conference on Information and Intelligent Systems—CECIIS, 23rd International Conference* (pp. 371–378). Faculty of Organization and Informatics.
- Galinec, D., & Steingartner, W. (2013). A look at observe, orient, decide and act feedback loop, pattern-based strategy and network enabled capability for organizations adapting to change. *Acta Electrotechnica et Informatica*, 13, 39–49.
- Gritzalis, D. (2021). *Cyber security and global information assurance: Threat analysis and response solutions*. Springer.
- Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley.
- Heikkilä, M., & Li, X. (2022). Cybersecurity risks in the age of digital transformation: A framework for organizational cyber resilience. *International Journal of Information Security and Privacy*, 16(1), 40–57.
- Herrington, L., & Aldrich, R. (2013). The future of cyber-resilience in an age of global complexity. *Politics*, 33(4), 299–310. <https://doi.org/10.1111/1467-9256.12035>
- Hong, J. (2020). A comprehensive review of cybercrime and cybersecurity challenges. *International Journal of Advanced Computer Science and Applications*, 11(12), 476–481.

- Huang, L., & Zhu, Q. (2021). Combating informational denial-of-service (IDoS) attacks: Modeling and mitigation of attentional human vulnerability. In *International Conference on Decision and Game Theory for Security* (pp. 314–333). Springer. https://link.springer.com/chapter/10.1007/978-3-030-90074-5_18
- Huang, L., & Zhu, Q. (2022). Radams: Resilient and adaptive alert and attention management strategy against informational denial-of-service (IDoS) attacks. *Computers & Security*, 121, 102844. <https://doi.org/10.1016/j.cose.2022.102844>
- Hu, Y., Tan, Z., & Zhao, X. (2023). Intelligent cybersecurity based on adaptive machine learning. *Journal of Intelligent & Fuzzy Systems*, 44(6), 5471–5482.
- Husain, S., & Khan, R. A. (2024). Towards a comprehensive understanding of cyber resilience: An interdisciplinary review. *Cybersecurity*, 7(1), 1–23.
- Institute for Cybersecurity and Society. (2024). *Cybersecurity best practices and governance*. University of Texas. <https://ics.utexas.edu/resources/cybersecurity>
- Kolokotronis, N., Shiales, S., Bellini, E., Charalambous, L., Kavallieros, D., Gkotsopoulou, O., Pavue, C., Bellini, A., & Sargsyan, G. (2019). Resilience and hybrid threats: Security and integrity for the digital world. In *IOS Press Ebooks*. <https://ebooks.iospress.nl/ISBN/978-1-64368-023-1>
- Kshetri, N. (2019). Cybersecurity and international political economy: Understanding global digital security challenges. *Third World Quarterly*, 40(4), 761–779.
- Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.
- Lewis, E., Burrell, D. N., Nobles, C., Ferreras-Perez, J., Richardson, K., Jones, A. J., & Jones, L. A. (2023). Cybercrime and cybersecurity challenges in the automotive industry utilizing agent-based modeling (ABM). In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 26). IGI Global. <https://doi.org/10.4018/978-1-6684-8846-7.ch008>
- Lohrke, F. T., & Frownfelter-Lohrke, C. (2023). Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *Journal of General Management*. <https://doi.org/10.1177/03063070231200512>
- MITRE Corporation. (2024). *ATT&CK framework for cybersecurity*. <https://attack.mitre.org>
- Moffett, J., & Desouza, K. C. (2023). Cybersecurity governance: Best practices for organizations. *QIT Press International Journal of Organizational Information Systems Development*, 5(1), 1–15. https://qitpress.com/articles/QITP-IJOIS_05_01_001
- Nair, S., & Ramachandran, M. (2024). Cybersecurity in smart cities: Challenges and solutions. *African Journal of Information Systems and Development*, 8(2), 33–44. <https://africansciencegroup.com/index.php/AJAISD/article/view/74>
- Nguyen, T. T., & Reddi, V. J. (2019). Deep reinforcement learning for cybersecurity. *arXiv preprint*. <https://arxiv.org/abs/1906.05799>
- Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies*, 16(3), 270–298. <https://doi.org/10.1080/14702436.2016.1196726>
- Rajivan, P., Janssen, M. A., & Cooke, N. J. (2013). Agent-based model of a cybersecurity defense analyst team. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 57(1), 100–104. <https://doi.org/10.1177/1541931213571069>
- Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep reinforcement learning for cybersecurity threat detection and protection: A review. *arXiv preprint*. <https://arxiv.org/abs/2206.02733>
- Thompson, B., & Morris-King, J. (2018). An agent-based modeling framework for cybersecurity in mobile tactical networks. *Journal of Defense Modeling and Simulation*, 15(1), 5–17. <https://doi.org/10.1177/1548512917738858>
- Vestad, A., & Yang, B. (2023). A survey of agent-based modeling for cybersecurity. In *Human Factors in Cybersecurity* (pp. 85–92). AHFE International. <https://openaccess.cms-conferences.org/articles/hfics-2023/085/>
- Walker, J., & Cooper, M. (2024). Cyber risk logics and their implications for cybersecurity. *International Affairs*, 100(6), 2441–2460. <https://doi.org/10.1093/ia/iiad092>
- Xu, S. (2020). Cybersecurity dynamics: A foundation for the science of cybersecurity. *arXiv preprint*. <https://arxiv.org/abs/2010.05683>
- Zhu, Q. (2024). Foundations of cyber resilience: The confluence of game, control, and learning theories. *arXiv preprint*. <https://arxiv.org/abs/2404.01205>
- Zhuang, Y., Li, Y., & Zhang, J. (2021). Agent-based modeling and life cycle dynamics of COVID-19-related online collective actions. *Complex & Intelligent Systems*, 7(3), 1451–1464. <https://doi.org/10.1007/s40747-021-00595-4>