Editorial for the Special Issue (2024): Network and Information Security in Cyber Systems

Mehmet Sahinoglu[1], Alberto Arteta[1], and Engin Maşazade[2]

[1]Department of Computer Science, Troy University, Troy, AL, USA
[2]Department of Electrical and Electronics Engineering, Marmara University, İstanbul, Turkey
Email: mesa@troy.edu (M.S.); aarteta@troy.edu (A.A.); engin.masazade@marmara.edu.tr (E.M.)
Manuscript received May 17, 2025; accepted May 19, 2025; published May 22, 2025

I. Introduction

In the 21st century, nations have increasingly engaged in covert cyberwars, particularly after the geopolitical shifts that followed the Cold War. While this battlefield spans national and local domains, it is the ever-growing incidence of fraudulent and malicious cyber activities driven by both technological gaps and complex legal ambiguities that continues to threaten the security, privacy, and financial stability of individuals, organizations, and governments alike. This is a massive, real, and existing challenge for scientists and researchers due to a lack of field data, the absence of international cooperation due to the politicization of this common enemy, and hidden privacy issues. Notwithstanding remarkable theoretical and applied advancements in cyber defense, the pace of emerging threats often outstrips the development of robust, scalable solutions. Researchers are challenged by a lack of accessible field data, fragmented international collaboration, and the delicate balance between privacy and surveillance. The financial stakes are steep. For instance, cybercrime reportedly cost the U.S. over $13.7 billion in 2018 alone. In response, the 2023 U.S. federal budget allocated nearly $11 billion for cybersecurity efforts, a testament to the urgency and magnitude of the problem. According to the European Cybersecurity Competence Center, EU will invest more than €760m in digital transition and cybersecurity (https://cybersecurity-centre.europa.eu).

II. Purpose of the Special Issue 2

This Special Issue 2 of the International Journal of Computer Theory and Engineering (IJCTE) aims to address this pressing global issue. It solicited original, unpublished research that not only investigated cyber- and information security threats and risks but also proposed practical, cost-effective mitigation strategies. Submissions of a political or strategic nature, particularly those with the potential to endanger the safety or digital sovereignty of individuals or nations, were excluded. The overarching objective of this issue is to inspire scientifically grounded, constructive solutions to unprecedented cybersecurity challenges. Rather than surrendering to the status quo or cyber extortionists, this initiative calls for proactive academic engagement. Contributions were expected to align with one or more of the following core themes:

1) Quantitative, Qualitative, and Hybrid Risk Assessment
2) Cost-Effective Risk Management and Cost-Benefit Analysis
3) Artificial Intelligence, Machine Learning, and Deep Learning
4) Probabilistic and Deterministic Problem-Resolution Approaches
5) Cloud Computing, Edge Computing, and Sensor Systems
6) Cryptology: Cryptography and Cryptanalysis
7) Blockchain and Cryptocurrencies, and Digital Banking
8) Neural Networks and Chaos Theory
9) Hacking, Malware, Ransomware, Firewalls, Virtual Machines, Digital Signatures
10) Cybersecurity in Outer Space, Naval, and Avionic Systems
11) Electronic, Telecommunication, and Electric Power Systems
12) Applications in Healthcare, Agriculture, and Government Systems
13) Digital Infrastructure, Internet of Things (IoT), and Net Piracy
14) Cybersecurity in Banking, Finance, Telemetry, and Telemedicine
15) Security in Renewable and Conventional Power Systems
16) Water Resources, Transportation, and Education
17) Defense, Research, and Industrial Infrastructure
18) National Infrastructure Vulnerability Database Risk Assessment and Optimal Management
19) Election Systems and Judicial Correctional Facilities
20) Highway and Railroad Cybersecurity Systems

III. Summary of Contributions

Special Issue 2 is a current collection of IJCTE journal publications [1–6] on the pivotal topic of Cybersecurity, following a modest closure of the Special Issue 1 on the then-popular COVID-19 and always mysterious and notorious Incurable Killer Diseases [7]. In chronological order from [1] to [6], the critical messages are outlined below to invite the audience to consider the articles in the archive of IJCTE. Note that the keywords from the onset have been employed partially or fully in the following six contributions addressing diverse aspects of cybersecurity:

[1, 2]: cover keywords: 1, 2, 4, 9, 17, 18
[3]: cover keywords: 5, 9
[4]: cover keywords: 4, 9
[5]: cover keywords: 5, 9
[6]: cover keywords: 6, 7, 9

IV. Highlights of Selected Articles

This section briefly summarizes the main contributions of each article included in the Special Issue. These highlights reflect the diverse approaches and innovations proposed by the authors to tackle critical challenges in cybersecurity as follows:

[1] Introduces the Defense Acquisition Risk Meter (DARM), a game-theoretic tool for quantitatively assessing and managing risk in defense procurement with cost and benefit.

[2] Proposes the Security Meter (SM) algorithm for risk quantification and cost-effective optimal risk management vis-à-vis Microsoft's EXCEL in national vulnerability databases.

[3] Presents a VM selection strategy using an updated Dragonfly Algorithm for improved energy efficiency.

[4] Focuses on Optimal Rule Ordering for firewalls using Particle Swarm Optimization.

[5] Evaluates green computing policies in cloud data centers and their impact on security performance.

[6] Introduces CP256-1299, a novel digital signature scheme based on cubic Pell curves since Elliptic Curve Cryptosystems proved to offer strong security with smaller key sizes.

V. Cross-Paper Comparative Analysis

This section provides a comparative overview of the six accepted articles in Special Issue 2. Table 1 below summarizes their distinct contributions, highlighting the domains addressed, methodologies applied, optimization tools used, and their relevance to key cybersecurity challenges:

Table 1. Cross-paper comparative analysis

Aspect	**[1, 2]**	**[3]**	**[4]**	**[5]**	**[6]**	**Common Themes**
Domain Focus	*National defense vulnerability*	*Cloud resource management*	*Network firewall security*	*Green cloud computing*	*Cryptographic security*	*Cybersecurity in critical systems*
Methodology	Game theory, LP optimization	Swarm intelligence	Particle Swarm Optimization	CloudSim simulation	Algebraic curve cryptography	Algorithmic innovation
Risk/Cost Trade-Off	Mitigation vs. risk exposure	SLA vs. energy	Latency vs. packet safety	Power vs. job completion	Key size vs. security	Performance trade-offs
Security Metrics	Security indices, vulnerability ranking	Migration success, SLA	Classification latency	Energy and delay rates	Signature strength	Quantitative benchmarks
Optimization Tool	SM, LP, Excel Solver	Dragonfly Algorithm	PSO + probability model	CloudSim toolkit	Custom ECC scheme	Risk-cost-performance
Scalability	Policy-level systems	Elastic cloud scaling	Dynamic firewall rules	Data center policy sets	Digital currency integration	Real-world deployments

VI. Conclusion

This editorial has summarized the main contributions in SI-2, emphasizing that cyber- and information security is no longer a siloed and underestimated, and overlooked IT issue but a critical national and global concern. The articles presented here aim to inform, inspire, and challenge the research community to continue innovating in the face of persistent digital threats. We believe this Special Issue 2 will help bridge the gap between theoretical advancement and practical implementation in cyber- and information security.

References

[1] M. Sahinoglu and J. C. Petty, "Quantitative risk assessment and management of national defense acquisition with a game-theoretic security risk meter tool," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 15, no. 4, pp. 152–177, 2023.

[2] M. Sahinoglu, "Cyber security risk assessment and optimal risk management of a national vulnerability database," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 16, no. 4, pp. 104–126, 2024.

[3] A. Prashar and J. Thakur, "An energy-efficient VM selection using updated dragonfly algorithm in cloud computing," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 16, no. 3, pp. 76–86, 2024.

[4] D. Hakani and P.S. Mann, "Enhanced particle swarm optimization-based approach to firewall optimal rule reordering," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 16, no. 4, pp. 134–144, 2024.

[5] K. Qureshi, A. Albusairi, and P. Manuel, "Empirical evaluation of virtual machine migration policies on power- and time-management in cloud computing," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 17, no. 2, pp. 83–90, 2025.

[6] N. A. Abu, A. Nitaj, and M. R. K. Ariffin, "A digital signature on cubic pell cryptosystem CP256-1299," *International Journal of Computer Theory and Engineering (IJCTE)*, vol. 17, no. 2, pp. 91–101, 2025.

[7] M. Sahinoglu and A. Arteta, "Editorial for the special issue (2022) on 'The recent advances in computer theory and software engineering on covid-19 pandemic and incurable killer diseases'," *International Journal of Computer Theory and Engineering (IJCTE),* vol. 15, no. 1, p. 61, 2023. doi: 10.7763/IJCTE.2023.V15.1331