The ISC Int'l Journal of Information Security
ISeCure

October 2025, Volume 17, Number 3 (pp. 1–8)
http://www.isecure-journal.org

Presented at the ISCISC'2025 in Tehran, Iran.

Mission-Centric Countermeasure Selection in Cybersecurity Situation Awareness Systems **

Sajed Yousefi Mashhour [1], Motahareh Dehghan [2], Babak Sadeghian [3,*]
Alireza Hashemi Golpayegani [3]

[1] *Department of Management, Science and Technology, Amirkabir University of Technology, Tehran, Iran.*
[2] *Department of Industrial Engineering, Tarbiat Modares University, Tehran, Iran.*
[3] *Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran.*

ARTICLE INFO.

Keywords:
Cybersecurity, Countermeasure Selection, Mission-Centric Security, Agent-Based Modeling, Multi-Criteria Decision Making

Type:

doi:

ABSTRACT

Selecting optimal cybersecurity countermeasures requires integration with mission-critical objectives beyond technical risk minimization. This paper presents a mission-centric framework for countermeasure selection in cybersecurity situation awareness systems by extending the RiskMAP methodology with agent-based and discrete-event simulation. The framework employs a multi-criteria decision-making approach based on the Confidentiality, Integrity, and Availability (CIA) triad, weighing mission objectives and mapping vulnerabilities and threats using MITRE ATT&CK and D3FEND taxonomies. Candidate countermeasures are evaluated considering risk reduction, implementation cost, operational impact, and mission alignment. We demonstrate the approach through a case study on a critical infrastructure organization's network modeled in AnyLogic. Results show improved alignment between security posture and organizational priorities while maintaining effective risk reduction, outperforming traditional methods. This framework enables quantitative visualization and optimization of security investments relative to mission continuity. All simulation models, data, and scripts are openly available to support reproducibility.

1 Introduction

Modern organizations increasingly rely on complex digital infrastructures to sustain their core missions, making them prime targets for sophisticated and persistent cyber threats. The challenge of safeguarding these environments extends beyond neutralizing technical vulnerabilities; security leaders must ensure that every defensive investment directly contributes to organizational priorities and operational continuity [1–3].

Traditional countermeasure selection methodologies frequently prioritize technical risk mitigation,

* Corresponding author.
**The ISCISC'2025 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: sajed.yousefi@aut.ac.ir, m_dehghan@modares.ac.ir, basadegh@aut.ac.ir, sa.hashemi@aut.ac.ir
ISSN: 2008-2045

cost efficiency, or regulatory compliance in isolation [4, 5]. However, such approaches often fail to account for the nuanced dependencies between security decisions and the broader organizational mission, leading to inefficient allocation of resources, operational disruption, and the potential erosion of mission-critical capabilities [6, 7]. Recent critiques emphasize that mission assurance must be tightly woven into cybersecurity planning to avoid such pitfalls [1, 2].

One substantial gap in contemporary practice lies in the limited integration of organizational objectives such as service continuity, business enablement, and resilience within cyber risk evaluation and countermeasure prioritization frameworks [6]. Existing solutions, including advanced risk assessment methods, offer value in systematic vulnerability identification and risk quantification but typically operate at a technical or operational layer, lacking mechanisms to translate business priorities into actionable security choices. Moreover, many defensive strategies rely on reactive controls, such as intrusion detection driven responses, which are vulnerable to evasion and often fail to prevent disruptions to mission-critical processes [7].

There is thus a critical need for a decision support paradigm that rigorously incorporates mission-centric objectives into the countermeasure selection process. Such a paradigm must not only evaluate technical efficacy but also quantitatively weigh the alignment of candidate controls with organizational priorities, model the propagation of risk through hierarchical asset dependencies, and balance preventive with reactive strategies in dynamic threat environments [5, 6].

Problem Statement: Despite notable advances, current cybersecurity situation awareness systems do not systematically support the selection of countermeasures that are optimally aligned with both risk reduction and the overarching mission objectives of the organization. Existing frameworks insufficiently capture the interplay between security interventions, business impacts, and operational dependencies, leading to suboptimal protection of mission-critical functions.

In response, this paper introduces a mission-centric countermeasure selection framework that extends the RiskMAP [8] methodology by embedding agent-based and discrete event simulation capabilities. Our approach integrates organizational priorities into all stages of analysis and maps threats and vulnerabilities to industry-standard taxonomies including MITRE ATT&CK and D3FEND [9–11] to ensure completeness and interoperability. Countermeasures are assessed using a multi-criteria decision making process grounded in the Confidentiality, Integrity, and Availability (CIA) triad, weighing risk reduction, implementation cost, operational impact, and mission alignment.

To demonstrate the effectiveness of this methodology, we apply it to a real-world critical infrastructure network, evaluating alternative countermeasures within a reproducible simulation-based case study. Our framework delivers actionable, quantitative support for aligning cybersecurity investments with mission assurance, addressing a longstanding gap in both academic research and operational practice.

The remainder of this paper is organized as follows: Section 2 reviews related work and identifies gaps in existing methodologies. Section 3 presents our mission-centric countermeasure selection framework, detailing hierarchical modeling, bidirectional propagation mechanisms, and multi-criteria evaluation. Section 4 describes the implementation and case study within a critical infrastructure organization using AnyLogic simulation. Section 5 presents comprehensive results including threat prioritization, countermeasure utility evaluation, and mission-level risk reduction achievements. Section 6 concludes with key contributions, practical implications, limitations, and future research directions. All simulation artifacts and analysis scripts are made available through our GitHub repository to ensure reproducibility and enable adaptation to diverse organizational contexts.

2 Related Work

Research on cybersecurity countermeasure selection has seen significant evolution, transitioning from static, risk-based models focused narrowly on patching vulnerabilities and minimizing technical risk, to more adaptive frameworks that integrate business context and resilience. Early countermeasure selection strategies primarily sought to minimize risk or cost without explicitly considering the impact of security actions on high-level organizational mission objectives [1, 3]. As Naspoli *et al.* [3] and subsequent surveys observed, these frameworks provided systematic methods to identify vulnerabilities and evaluate mitigation options but rarely modeled the effects of interventions on business operations, leading to frequent decision-making blind spots and potentially unintended consequences.

The absence of organizational context in earlier models led to the emergence of mission-centric critiques, notably articulated by Endsley [1], who stressed that effective cyber situational awareness requires continuous alignment of security decisions with evolving organizational priorities. Without this alignment, even technically robust solutions may result in inefficient resource allocation, operational

disruption, or weakened mission assurance.

2.1 Dynamic and IDS-Centric Approaches

With the diversification of cyber threats, dynamic countermeasure selection systems have become prominent. These approaches typically center on Intrusion Detection Systems (IDS), orchestrating automated responses upon threat detection [7, 12]. Such systems operate in near real-time, leveraging alert data from IDS/IPS deployments to recommend or enact appropriate countermeasures. For instance, automated intrusion response frameworks [7] rapidly deploy mitigating controls to contain ongoing attacks, thus minimizing the window of exploitation.

Nonetheless, IDS-centric strategies exhibit notable shortcomings. Attackers increasingly employ advanced evasion techniques to circumvent detection, thus limiting the efficacy of reactive, alert-driven security management. Furthermore, large-scale or complex infrastructures generate volumes of IDS data that can overwhelm operators and introduce noise [4]. The computational cost associated with maintaining up-to-date attack models, as well as the inherent delays and false positives in detection pipelines, pose risks to timely and appropriate intervention.

2.2 Optimization and Attack Graph-Based Models

Parallel to IDS-centric approaches, the cybersecurity literature has explored optimization-driven models for defense planning. Attack graphs and multi-path response frameworks formalize the relationship between potential attack sequences and available security controls using mathematical structures [4, 5]. By casting countermeasure selection as a resource allocation or coverage problem, these models seek to maximize system resilience within practical budgetary or operational constraints.

Li *et al.* [5] introduced the "attack coverage surface" metric, using optimization techniques to identify cost-effective sets of defenses. Viduto *et al.* [4] proposed multi-criteria optimization models to facilitate holistic decision support for countermeasure selection. While such methods offer rigorous protection in simulated or small-scale environments, they are highly sensitive to model assumptions and can become computationally infeasible as system complexity grows.

A key limitation of these frameworks is their continued dependence on accurate, timely threat intelligence—often sourced from IDS or vulnerability scans [13]—as well as their focus on reactive rather than preventive controls. The need for scalable, proactive decision support remains critical.

2.3 Preventive and Decision Support Approaches

To address scalability and shift the focus toward preemption, recent work has developed decision-support systems aimed at optimizing the selection of preventive countermeasures. These systems incorporate structured processes—often leveraging multi-criteria decision-making or hybrid analytic methods—to align security investments with risk posture, operational constraints, and resource availability [6, 14].

For example, Sönmez *et al.* [6] constructed a decision-support methodology that integrates quantitative risk metrics with budgetary limitations to recommend preventive controls. Other frameworks have introduced multi-layered information models and agent-based techniques to simulate the cascading effects of risk propagation and mitigation across organizational hierarchies [14]. However, these approaches frequently lack the flexibility to rapidly adapt to emerging threats and may not fully support dynamic reprioritization based on real-time mission changes.

2.4 Gaps and Advances Motivating This Work

Three persistent gaps are evident in the literature: (1) insufficient consideration of the explicit organizational mission in countermeasure selection, leading to suboptimal alignment between information security and business objectives; (2) the scalability limitations of attack-path and optimization-based methods in large-scale or real-world environments; and (3) the overemphasis on reactive mitigation rather than preventive, mission-oriented measures [4, 5, 7].

To address these gaps, recent research—including work by FarahaniNia *et al.* [15] and Dehghan *et al.* [16]—has proposed multi-level models and simulation-based evaluation as means of linking technical risk indicators to organizational impact. The adoption of internationally recognized taxonomies, like MITRE ATT&CK [9] and D3FEND [10], further enhances coverage and interoperability across enterprises.

This paper advances the state of the art by delivering a mission-centric, simulation-enabled decision support framework that (i) formalizes the integration of organizational objectives, (ii) utilizes hybrid agent-based and discrete-event modeling to quantify the system-wide effects of security measures, and (iii) achieves empirically validated gains in mission alignment and risk mitigation in a complex, real-world case. Comprehensive benchmarking and transparency are ensured through the open release of all simulation code and supporting artifacts.

3 Mission-Centric Countermeasure Selection Framework

The proposed framework is constructed around a hierarchical, bidirectional process explicitly designed to align security investments with organizational mission priorities. The core workflow comprises: *(1) top-down propagation of mission weights via the CIA triad*, *(2) bottom-up threat risk propagation and aggregation*, *(3) prioritized threat identification*, *(4) utility-based countermeasure selection*, and *(5) simulation-driven evaluation of risk reduction.*

3.1 Information Acquisition and Hierarchical Modeling

The process begins with the structured documentation of mission objectives. *Each mission objective is assigned specific weights for confidentiality (w_C), integrity (w_I), and availability (w_A), **such that in each dimension, the sum of all mission objectives' weights is 1:***

$$\sum_{k=1}^{K} w_C^{(k)} = 1, \quad \sum_{k=1}^{K} w_I^{(k)} = 1, \quad \sum_{k=1}^{K} w_A^{(k)} = 1,$$

where K is the number of mission objectives.

Organizational tasks supporting these objectives are identified and mapped. Subsequently, key assets are catalogued—including their roles and dependencies—followed by up-to-date vulnerability information. Threats are mapped to vulnerabilities using the MITRE ATT&CK framework [9]; potential countermeasures are mapped using MITRE D3FEND [10]. This establishes a hierarchical database: mission objectives → tasks → assets → threats/vulnerabilities → countermeasures.

3.2 Risk Assessment

The risk assessment proceeds through three core computational processes, detailed as follows.

3.2.1 Top-Down Weight Propagation

Mission objective CIA weights are propagated downward through the organizational hierarchy and their related dependencies. Each task and asset inherits the CIA importance profile of the mission(s) it supports, with proper normalization at each level. This ensures risk calculations downstream fully reflect mission priorities.

3.2.2 Bottom-Up Risk Propagation

For every threat, risk scores are initially determined (using, e.g., CVSS for vulnerabilities). These scores are then aggregated upward, from assets to tasks and ultimately to mission objectives, via the structure of dependencies established in the model.

3.2.3 Threat Prioritization

For each threat, a **priority score** is computed by multiplying its initial risk (inferred from vulnerability data) by the propagated CIA weights from the mission objectives it endangers:

$$\text{Priority Score}_i = \text{Risk}_i \times \sum_{d \in \{\mathcal{C},\mathcal{I},\mathcal{A}\}} W_{\text{i}}^{(d)}$$

where W_i is the normalized weight of threat i.

The threats with the highest priority scores (i.e., those posing the greatest risk to mission-critical functions) are selected for further countermeasure analysis.

3.3 Countermeasure Selection and Utility-Based Evaluation

For each prioritized threat, candidate countermeasures (sourced via MITRE D3FEND) are retrieved. Their effectiveness is rigorously assessed using a multi-criteria utility score, denoted CMU, incorporating the following:

- **Target Threat Risk Reduction (RR_{tt}):** The expected reduction in risk for the targeted threat following countermeasure deployment.
- **Implementation Cost (C):** Total deployment cost, including direct and indirect expenses.
- **Negative Impact on Service Quality (Q):** Any negative effects on performance, availability, or usability.
- **Non-Target Threat Risk Reduction (RR_{nt}):** Additional risk mitigation effects on other (non-targeted) threats.

The utility score for countermeasure j is:

$$\text{CMU}_j = w_1 \cdot RR_{tt}(j) - w_2 \cdot C(j) - w_3 \cdot Q(j) + w_4 \cdot RR_{nt}(j)$$

where $w_{1,2,3,4}$ are organization-specified weights reflecting mission preferences and constraints.

After utility scores are calculated, the countermeasure(s) with the highest CMU values are selected. The simulation model then proceeds to simulate deployment of these countermeasures.

3.4 Simulation

Upon "deploying" the selected countermeasures in the AnyLogic simulation model, the framework repeats the bottom-to-top risk propagation and aggregation, capturing updated (residual) risk values for all assets, tasks, and mission objectives. This enables explicit

quantification of achieved risk reduction, holistic estimation of any negative operational impacts, and direct visualization of impacts on mission assurance.

4 Implementation and Case Study

To empirically validate the proposed mission-centric countermeasure selection methodology, we conducted an implementation and case study within a critical infrastructure organization, utilizing agent-based and discrete-event simulation capabilities of the AnyLogic [17, 18] platform. The case study institution's environment encompassed three primary mission objectives—service deployment, enhancement, and security assurance—which were initially documented and assigned specific weights across the confidentiality, integrity, and availability (CIA) triad. This process followed our information acquisition framework, ensuring that for each CIA dimension, the sum of the weights across all mission objectives equaled unity, thereby accurately reflecting the relative importance of each objective in the overall organizational context.

Comprehensive data collection was then performed to enumerate operational tasks supporting each mission objective, map dependencies, and catalog critical assets together with their operational contexts and vulnerabilities. Figure 1 illustrates the organization's network topology, displaying the arrangement and interconnections among mission-critical servers, network infrastructure; this representation was essential for accurately modeling asset dependencies, risk propagation, and the structural context required for countermeasure analysis.

Building upon the established infrastructure mapping, we executed a thorough vulnerability scan to derive asset risk profiles [19, 20], and systematically mapped threats to vulnerabilities using the MITRE ATT&CK framework, thereby ensuring a comprehensive and standardized approach to adversarial tactics identification. In parallel, candidate countermeasures were enumerated and mapped using the MITRE D3FEND knowledge base, focusing this taxonomy explicitly on the available defensive measures rather than threat categorization. All hierarchical input data—including CIA weights, asset attributes, threat mappings, and countermeasure specifications—were formally encoded into the simulation model to support rigorous, reproducible computational analysis.

With this foundation, the simulation proceeded to implement the core bidirectional computational flows central to our methodology. Initially, mission objective CIA weights were propagated in a top-down manner throughout the organizational hierarchy, ensuring that each task, asset, and their subsidiary nodes expressed the inherited mission priorities for each security dimension. Subsequently, a bottom-up risk propagation was performed: risk values were aggregated upward from assets to tasks and mission objectives according to dependencies established in earlier phases. Threat prioritization was accomplished by multiplying each threat's risk score by the relevant propagated CIA weights, enabling precise computation of the impact of each adversarial action on organizational priorities. The model then selected the highest-priority threats based on these composite priority scores.

For those prioritized threats, candidate countermeasures were evaluated using a comprehensive utility function that integrated multiple criteria—including target threat risk reduction, cost of implementation, negative impact on quality of service, and risk reduction for non-target threats—thereby providing a nuanced, organizationally aligned basis for selection. Countermeasures attaining the highest utility scores were virtually deployed within the simulation environment, after which the model recalculated the resulting changes in residual risk, aggregating updated risk values from bottom to top and allowing direct measurement of mission-level risk reduction.

This thorough, end-to-end process established a robust evidence base for quantitatively assessing the framework's effectiveness. The simulation-driven findings confirmed that the mission-centric methodology delivered superior risk reduction and alignment with organizational goals compared to conventional technical- or cost-focused methods, validating the practical value of our approach in supporting informed, impactful cybersecurity decision-making in complex real-world settings.

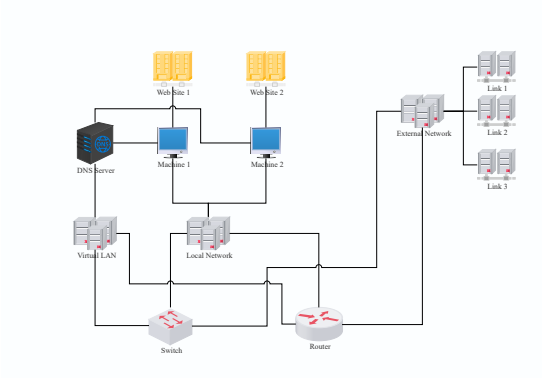

Figure 1. Organizational Network Topology employed in the case study.

5 Results and Discussion

The results from our case study empirically validate the effectiveness of mission-centric countermeasure selection in producing actionable, resource-efficient, and business-aligned security recommendations.

5.1 Threat Prioritization and Mission Impact

The first major output of the hybrid simulation was a prioritized threat landscape grounded in both technical exposure and organizational mission weighting. Table 1 displays the computed priority scores for all significant threats. The scoring algorithm incorporates the propagated Threat CIA weights, and threat risk (based on CVSS scores), synthesizing these according to our multi-level model.

Table 1. Threat Priority Scores

Threat ID	Threat Name	Priority Score
Th3	Unauthorized Access	74.17
Th7	Birthday Attack	49.47
Th2	Remote Code Execution	39.28
Th1	Server-Side Request Forgery (SSRF)	22.88
Th5	Spoofing Attacks	11.27
Th6	Plaintext-recovery attacks	7.13
Th4	Downgrade of DH parameter curves to export strength	5.45

As indicated, Th3 demonstrates the highest priority (74.17), overwhelmingly influencing the organization's mission-centric risk, followed by Th7 and Th2. This prioritization not only reflects technical severity, but validates mission-weighted aggregation by identifying those threats whose mitigation generates the largest reduction in overall mission risk.

5.2 Countermeasure Utility Evaluation

Subsequent simulation steps evaluated each countermeasure's expected contribution to mission risk reduction, cost, and operational effect. Table 2 reports the multi-criteria utility scores for all candidate countermeasures as ranked by the selection algorithm.

Table 2. Countermeasure Utility Scores. "CM ID" is the Countermeasure ID, and "Score" is the calculated CM Utility Score.

CM ID	Countermeasure Name	Score
CM6	Apply the latest fixes of OpenSSL	25.08
CM8	Implement strong access controls	22.93
CM10	Educate users	21.71
CM7	Upgrade to supported versions of OpenSSL	19.86
CM9	Monitor network traffic	18.80
CM5	Implement Network Segmentation	17.12

Countermeasure CM6 (e.g., OpenSSL update/fix) yields the highest utility score (25.08), balancing risk reduction, threat coverage, cost, and side-effect minimization. High utility scores for other countermeasures (CM8, CM10) arose from supplementary effectiveness or relatively low operational burden, yet these did not surpass the cost-benefit ratio of CM6.

Table 3. Empirical evaluation of countermeasures for Threat 3. CM = Countermeasure, Red. = Reduction, B/C = Benefit/Cost, Conf. = Confidentiality, Integ. = Integrity, Avail. = Availability.

CM	Cost	Risk Reduction (%)			Avg.	B/C
	(USD)	Conf.	Integ.	Avail.	Red.	
CM6	100	87	87	87	87.0	0.870
CM10	500	87	87	87	87.0	0.174
CM7	500	86	85	85	85.3	0.171
CM9	1000	88	89	89	88.7	0.089
CM8	1000	88	87	87	87.3	0.087
CM5	3000	89	90	90	89.7	0.030

Table 3 provides a detailed breakdown of each countermeasure's cost, risk reduction per CIA dimension, overall average risk reduction, and computed benefit-to-cost ratio for Th3. CM6 stands out, not just in utility score but also in superior cost-effectiveness, demonstrating an 87% average risk reduction at minimal resource expenditure.

5.3 Mission-Centric Risk Reduction

The cumulative impact of deploying the top-ranked countermeasures was assessed at the mission-objective level. Table 4 details risk reduction percentages across all mission objectives and CIA dimensions.

Table 4. Risk Reduction Percentages by Mission Objective. Conf. = Confidentiality, Integ. = Integrity, Avail. = Availability.

Mission Objective	Avail. (%)	Integ. (%)	Conf. (%)
Service Deployment	97	97	97
Service Enhancement	85	85	82
Security Assurance	89	89	87

Deployment of optimal controls led to a 97% reduction in risk for all CIA dimensions in the "Service Deployment" objective, with strong, quantifiable reductions in "Service Enhancement" and "Security Assurance" as well (82-89%). These results surpass those typically observed with technical- or cost-only prioritization methods. They clearly demonstrate the

amplifying effect of aligning cybersecurity interventions with organizational missions; the cascading benefits accrue at the highest-priority business layers, not merely at the technical perimeter.

6 Conclusion and Future Work

We have presented a mission-centric, simulation-driven framework for cybersecurity countermeasure selection, bridging the enduring gap between technical risk management and business-driven security objectives. By leveraging agent-based and discrete-event simulation models rooted in the CIA triad, and by systematically mapping mission objectives through assets and threats to countermeasures via established taxonomies (MITRE ATT&CK, D3FEND, CVE), the approach empowers organizations to select not just technically effective, but mission-critical and resource-efficient solutions.

Empirical validation in an operational environment evidences the superiority of this approach: up to 97% risk reduction was achieved across all mission-critical objectives (see Table 4), with transparent, high-utility, and cost-effective countermeasure recommendations (Tables 2 and 3). The methodology enables informed trade-off analysis, directly visualizes impact on business outcomes, and robustly supports adaptation to real-time threat and asset changes.

The main practical limitation remains the reliance on detailed, current asset/dependency mapping and expert-guided mission weighting, which may challenge rapid scaling for some organizations. Ongoing and future research will address these via integration of automated asset discovery, dynamic threat intelligence feeds, and AI-guided weight elicitation to further streamline the methodology. Extensive cross-sector and cross-organizational validation is underway to confirm the generality and resilience of the recommendations.

In sum, the mission-centric approach offers a reproducible, actionable, and business-aligned path to robust cyber defense, equipping organizations to maximize the impact of their security investments while ensuring sustained mission assurance in the face of evolving cyber threats.

Acknowledgment

The authors gratefully acknowledge the organizational collaborators, cybersecurity analysts, and IT staff who provided critical insight, data, and validation support for this research. Special thanks are extended to the AnyLogic simulation modeling community for technical guidance, particularly in agent-based and discrete-event framework implementation.

Availability of Data and Materials

All simulation models, code, and supporting datasets used in this study—including the AnyLogic project, modeling scripts, countermeasure evaluation data, and technical documentation—are freely available at: https://github.com/sajious/ABM-DES_RiskMap. The repository is organized for reproducibility, offering case study artifacts, raw and processed data, analytical scripts, and instructions for replicating results or adapting the methodology to alternate organizational settings, in alignment with open research principles and IEEE conference policy.

References

[1] M. R. Endsley. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 1995.

[2] H. Tianfield. Cyber Security Situational Awareness. In *Proceedings of the 2016 IEEE International Conference on Internet of Things*, 2016.

[3] P. Nespoli, D. Papamartzivanos, F. Gómez Mármol, and G. Kambourakis. Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. *IEEE Communications Surveys & Tutorials*, 2018.

[4] V. Viduto, C. Maple, W. Huang, and D. López-Peréz. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, 2012.

[5] F. Li, Y. Li, S. Leng, Y. Guo, K. Geng, Z. Wang, and L. Fang. Dynamic countermeasures selection for multi-path attacks. *Computers & Security*, 2020.

[6] F. Ö. Sönmez and B. G. Kılıç. A Decision Support System for Optimal Selection of Enterprise Information Security Preventative Actions. *IEEE Transactions on Network and Service Management*, 2021.

[7] A. Shameli-Sendi, H. Louafi, W. He, and M. Cheriet. Dynamic Optimal Countermeasure Selection for Intrusion Response System. *IEEE Transactions on Dependable and Secure Computing*, 2018.

[8] J. Watters, S. Morrissey, D. Bodeau, and S. C. Powers. The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues. Technical report, 2009.

[9] MITRE ATT&CK Framework. [Online], 2024. Available: https://attack.mitre.org/ [Accessed: May 2024].

[10] MITRE D3FEND Knowledge Graph. [Online], 2024. Available: https://d3fend.mitre.org/

[Accessed: May 2024].
[11] Common Vulnerabilities and Exposures (CVE). [Online Database], 2024. Available: https://www.cve.org/ [Accessed: May 2024].
[12] A. Shameli-Sendi and M. Dagenais. ORCEF: Online response cost evaluation framework for intrusion response system. *Journal of Network and Computer Applications*, 2015.
[13] Nessus Vulnerability Scanner. [Software]. Available: https://www.tenable.com/products/nessus.
[14] A. Mahdavi. *The Art of Process-Centric Modeling with AnyLogic*. AnyLogic Company, 2019.
[15] S. FarahaniNia, B. Sadeghiyan, M. Dehghan, and S. Niksefat. Impact Assessment for Cyber Security Situation Awareness. *International Journal of Information & Communication Technology Research*, 15(3), 2023.
[16] M. Dehghan, A. Mahdi Zadeh, and B. Sadeghian. A Model to Measure Effectiveness in Cyber Security Situational Awareness. *Computer and Knowledge Engineering*, 7(1):17–26, 2024.
[17] AnyLogic: Multimethod Simulation Software. [Software]. Available: https://www.anylogic.com/.
[18] I. Grigoryev. *The Big Book of Simulation Modeling: Multimethod Modeling with AnyLogic 6*. AnyLogic North America, 2013.
[19] ISO/IEC 18033: Information technology – Security Techniques – Encryption algorithms, 2015.
[20] NIST Special Publication 800-56C Revision 2: Recommendation for Key Derivation through Entropy Extraction and Expansion. Technical report, National Institute of Standards and Technology, April 2020.

Sajed Yousefi Mashhour is a Research Assistant at Amirkabir University of Technology. He earned his Master of Science in Information Technology Engineering from Amirkabir University of Technology in 2024, after completing his Bachelor of Science in Railway Mechanical Engineering from Iran University of Science and Technology in 2020. His research interests include Countermeasure Selection, Cybersecurity Situational Awareness Systems, Agent-Based Modeling, Cybersecurity, Intrusion Response Systems, Threat Modeling, and Risk Management.

Motahareh Dehghan is an Assistant Professor in the Department of Industrial and Systems Engineering at Tarbiat Modares University. She earned her Ph.D. in Information Security from Amirkabir University of Technology. Her research interests include Information Security, Cybersecurity Situational Awareness, and Emerging Technologies, focusing on developing innovative solutions to enhance Digital Security and Resilience.

Babak Sadeghian received his Ph.D. in Computer Science from University College, University of New South Wales, Australia, in 1993. Since then, he has joined as a faculty member of the Department of Computer Engineering at Amirkabir University of Technology, Tehran, Iran. His research interests include all aspects of Information Security. His current research interests include Intrusion Detection Systems, Cybersecurity Situational Awareness, Threat Hunting, Privacy Issues, Digital Forensics and Vulnerability Analysis.

Alireza Hashemi Golpayegany is an Assistant Professor in the Department of Computer Engineering at Amirkabir University of Technology, Tehran, Iran. His research interests include financial fraud detection, blockchain security, social commerce, business process mining, and recommender systems, with particular focus on developing intelligent systems for enhancing security and trust in digital platforms.