

SIMULATION ANALYSIS OF THE STRUCTURAL IMPACT OF AI AMPLIFIERS ON GLOBAL CYBER RISK MAPS

Yoana Ivanova

Department of Telecommunications, New Bulgarian University
Bulgaria

Corresponding Author, e-mail: yivanova@nbu.bg

Abstract: The aim of this paper is to present a simulation-based analysis of the structural impact of conceptual AI amplifiers on Global Cyber Risk Maps for 2023-2025. NetLogo was preferred by the author for the practical part of the study because of its advantages and suitability for creation of conceptual models of a wide variety of complex systems. The results are presented for different simulation scenarios, including one in which AI amplifies cyber protection and another in which it amplifies cyberattacks. Consequently, this experimental research contributes to a better understanding of how AI amplifiers affect cyberattack mechanisms and effective strategies for strengthened prevention.

Key words: Global Cyber Risk Maps cyberattack AI technologies simulation model cyber.

1. INTRODUCTION

The Global Cyber Risk Maps provide basic data for continuously updating conceptual simulation models that visualize the impact of cyberattacks on governance structures. In the Global Risks landscape, the cyber “nodes” are represented by “*Widespread cybercrime and cyber insecurity*” (2023) [1], “*Cyber insecurity*” (2024) [2], and “*Cyber espionage and warfare*” (2025) [3]. Typical examples of widespread cybercrime and cyber insecurity (WCCI) include *DDoS (Distributed Denial of Service) attacks, phishing and social engineering, malware, ransomware, and cyber espionage*.

As cyber espionage is a subcategory of WCCI, all relevant cyber nodes in the simulation models described in the practical part of the study are defined as “WCCI”, serving as the primary conceptual input for assessing the impact of AI (Artificial Intelligence) amplifiers.

The AI nodes are introduced for the first time in the 2024 diagrams, labeled as “*Adverse outcomes of AI technologies*”. This means that, on one hand, AI can be used by hackers to automate phishing campaigns, accelerate the detection of system vulnerabilities, or execute complex DDoS attacks. On the other hand, AI functionalities can contribute to reinforcing cyber defense mechanisms in the network. In their defensive role the AI technologies are capable of enabling automatic cyberattack

detection, vulnerability prediction, real-time countermeasures, and steganographic protection of sensitive data. It should be noted that steganographic data embedding can be used not only by defenders, but also by attackers. For example, artificial neural networks based on the backpropagation of error algorithm are capable to identify modifications in the original data.

According to the summarized information, based on the World Economic Forum's Global Risks Reports, cyber insecurity has been ranked among the most serious global risks during the period from 2023 to 2025. For example, in 2024 it was identified as a high global risk, including malware, deepfakes, and misinformation threatening supply chains. Additionally, by 2025, 72% of cyber leaders reported increasing cyber risks. Therefore, the persistent escalation of cyber insecurity and the growing influence of AI technologies underline the necessity for simulation-based research related to analyzing the structural impact of AI amplifiers within global cyber risk maps.

The study is organized into two sections. Section 2, titled "Related Work", describes the conceptual framework of a referenced simulation model, adapted by the author for the most recent Global Risks Maps. Section 3 presents the essentials of the experimental study conducted, including modeling an extended simulation model, as well as the assessment and analysis of results.

2. RELATED WORK

In this section, the fundamental principles of the research methodology are presented together with a brief review of the state-of-the-art. The presented experimental research is scientifically grounded as an extension of the author's previous research, based on a relevant reference simulation model titled "*Cyber Threats to Global Governance*" [4]. This simulation model of a cyberattack against a global governance structure is created using data from the *Global Risks Report 2012 (Seventh Edition)* [5]. The global risks are represented by nodes which are interconnected by links for analysing the propagation of cyber threats toward a central governance entity.

Agent-based simulation modeling is a flexible method for representing complex systems by allowing multiple relationships among agents. The simulation framework enables generating shortest paths between individual risk nodes and governance structures. It should be noted that this model can be used as a suitable baseline for further extensions and comparative studies across different time periods, because of its valuable concept, clarity and adaptability. The first modification of the original simulation model introduced by the author of the present research is based on the *Global Risks Report 2015 (Tenth Edition)* [6] and is adapted to investigate a cyberattack against a management structure.

The present study aims to extend the previous research by incorporating conceptual AI amplifiers into simulation models to illustrate the key role of these advanced technologies in cyberattack propagation, based on recent global cyber risk maps (2023-2025). The models vary key input parameters, such as attack duration, intensity, and target location. This study presents a complementary analytical perspective, enabling comprehensive risk assessment and analysis.

From a fundamental perspective, the main concepts of classical shortest-path

algorithms are provided by graph theory. They have been described in various studies related to network analysis, risk propagation modeling, and complex networks. For example, the scientific article entitled “*A Performance Comparison of Shortest Path Algorithms in Directed Graphs*” [7] examines several widely used algorithms for solving shortest-paths problems in directed graphs. Mathematically, shortest-path algorithms such as Dijkstra’s, Dantzig’s, Bellman-Ford, and Floyd-Warshall aim to minimize the cumulative edge weight along a path in a graph depending on the graph structure, size, and density [8].

It should be noted that classical shortest-path algorithms are intentionally not implemented in the program code of the original simulation model. This is because the network is designed to be conceptual and structure-driven, where shortest paths are represented by predefined morphic chains based on expert semantic Global Risk Maps, and no real edge weights are available for algorithmic optimization. In this sense, this is not a limitation of the model, but rather a sophisticated design solution. In this case, shortest paths are visually distinguished by a color-coding scheme (white, yellow, cyan) that reflects different propagation pathways, allowing the conceptual network to illustrate risk propagation effectively.

The reference simulation model (created in the simulation software NetLogo [9]), based on the original cited simulation model “*Cyber Threats to Global Governance*”) and 2023 Global Risks Map of cyber threats (Fig. 1), is shown in Fig. 2. The rationale for including this model in the Section 2 “Related Work” is that, with the exception of basic architectural changes related to the renaming of nodes and the links between them, it does not introduce additional commands in the program code and does not extend the method proposed by the original author. However, these basic architectural modifications are necessary for subsequent work on modeling an extended simulation model, which is presented in Section 3.

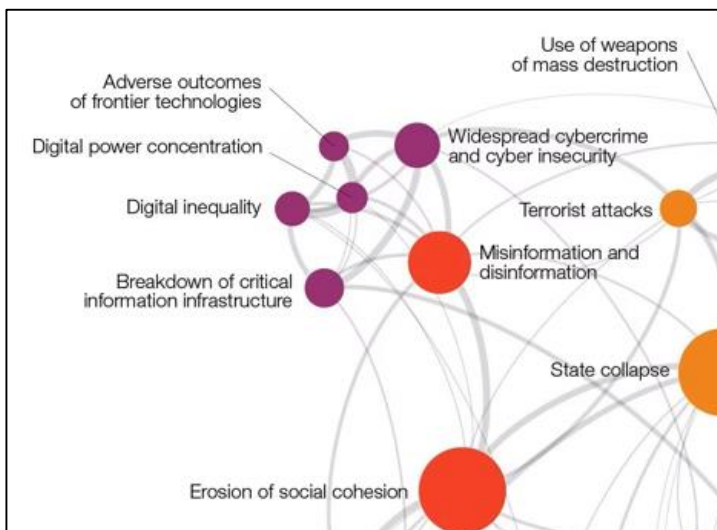


Fig. 1. A part of the 2023 Global Risks Map of cyber threats.

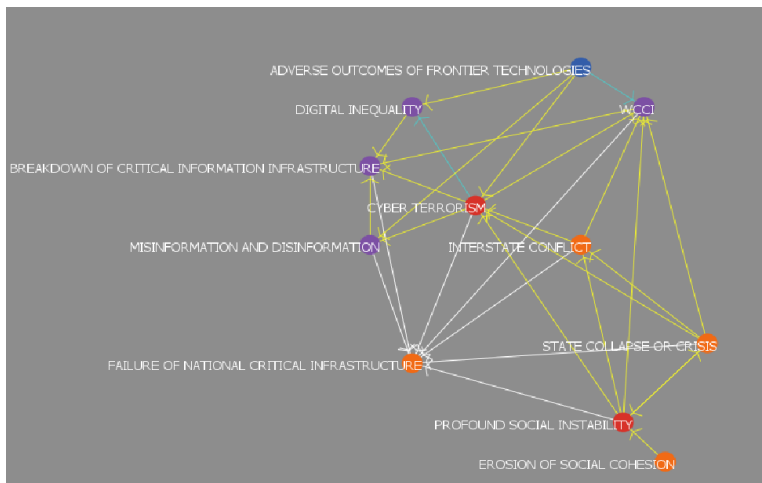


Fig. 2. A reference simulation model, based on the original cited simulation model “Cyber Threats to Global Governance”.

Recent literature has used network, cascade, and agent-based models to examine how cyber risks propagate through interconnected systems. Several studies demonstrate that AI can amplify both cyber-attacks and defense strategies. It is possible to multi-agent frameworks and Markovian modeling to simulate interactions between cyber-attackers and cyber-defenders in network systems [10]. For example, the innovative “game-theoretic approaches have modeled attacker-defender interactions in cyber systems, applying adaptive strategies “under uncertainty” [11], while “Multi-Agent Reinforcement Learning (MARL) has shown great potential as an adaptive solution for addressing modern cybersecurity challenges” [12].

3. MODELING AN EXTENDED SIMULATION MODEL TO STUDY THE IMPACT OF AI AMPLIFIERS

This section introduces the practical part of the study, focusing on the extension of the simulation model shown in Fig. 2, aimed at improving its accuracy and functionality. It should be noted that the node titled “Adverse outcomes of frontier technologies”, represents a preliminary variant of “Adverse outcomes of AI technologies” used in the simulation model, based on aggregated information from the 2024/2025 Global Risks Maps of cyber threats (Fig. 3). It is important to be explained that in the improved simulation model, the node titled “Erosion of social cohesion” has been renamed to “Erosion of human rights” to reflect a more specific aspect of social instability, conceptually linked to the main node “Profound social instability”.

In fact, the program code of the reference model was updated with new commands in order to amplify the adverse effects of AI technologies. The additional commands are included and described in Table 1, while the modified simulation model is presented in Fig. 4. The key modifications include new links between the nodes, *ai-weight* multipliers, and the normalized AI-risk plot. In fact, the main logic is that when the *ai-weight* of the adverse effects of the impact of AI-technologies increases, the

corresponding risk intensity also increases. Therefore, when the *ai-weight* is equal to 0, the risk intensity reaches its minimum based on the assumption that in this case cyber protection is at its maximum and the adverse effects are reduced. This means that the AI-technologies contribute to effective cyber protection when *ai-weight*=0, demonstrating the dual role of AI in the simulation model.

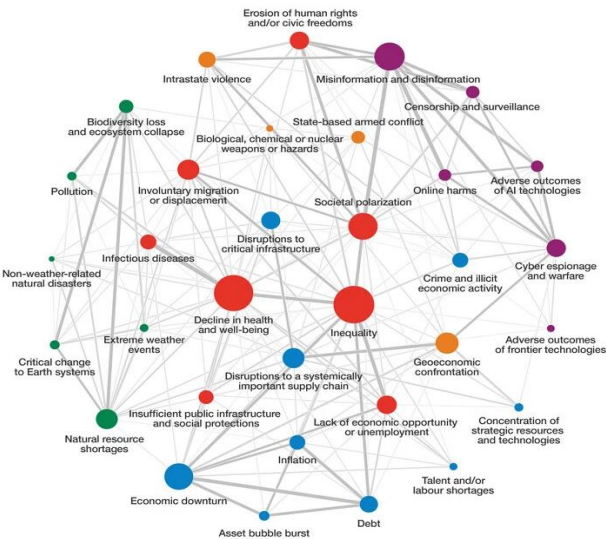


Fig. 3. The Global Risks Maps of cyber threats for 2025.

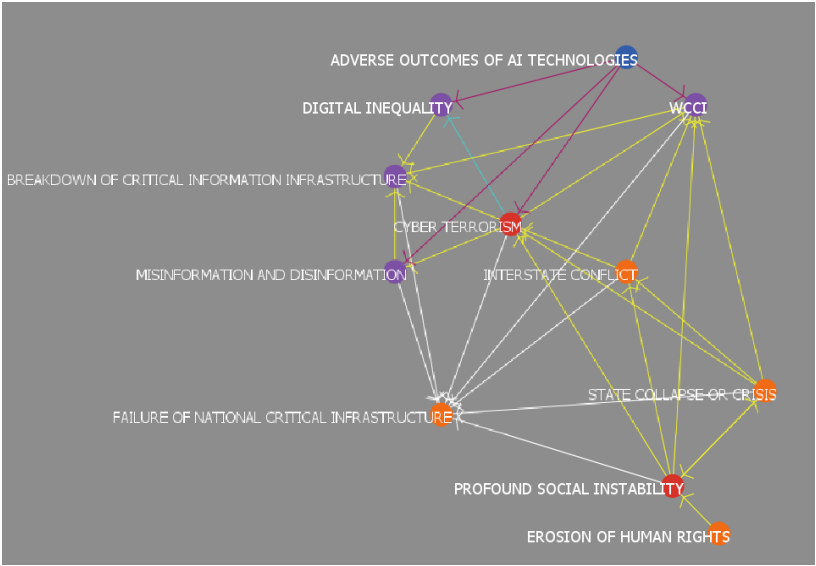


Fig. 4. A modified simulation model, based on the 2024/2025 Global Risks Maps of cyber threats.

Table 1.

<i>Description of code modifications</i>	<i>Modifications in the program code</i>
Global variables for path counts and AI amplification	globals [path-one-chain path-two-chain path-three-chain path-four-chain total links ai-amplifier]
Set AI-amplifier value	to setup set ai-amplifier 0-5
Applying AI effects and collect statistics	to draw-network apply ai-amplification statistics
Counting AI-amplified links Plotting AI-amplified risk in normalized format	to statistics set path-four-chain count links with [color magenta] set-current-plot-pen “4 AI-Amplified Chain” plotxy 4 path-four-chain/ total links set-current-plot “4 AI-Amplified Chain” set-current-plot-pen “AI Risk” plot sum [ai-weight] of links
Creating cyber threat links with risk weights and AI-weights	to cyber-threats-web create-link-to-turtle 0 [set color white set risk weight 1 set ai-weight 1] create-link-to-turtle 1 [set color yellow set risk weight 1 set ai-weight 1] create-link-to-turtle 2 [set color yellow set risk weight 1 set ai-weight 1] create-link-to-turtle 3
Defining frontier tech node, set label, and create AI-weight	to frontier-tech-threats-web set label risk-situation create-link-to turtle 3 [set color magenta set risk-weight 1 set ai-amplifier] create-link-to turtle 5 [set color magenta set risk-weight 1 set ai-amplifier]
Applying AI-amplification dynamically along links	to apply-ai-amplification ask turtles with [risk-situation = “Adverse outcomes of AI technologies”] ask my-links [set ai-weight ai-weight * ai-amplifier set color magenta]

The baseline model, which served as the foundation for the modification presented in this paper, is available and cited correctly under reference [4]. The modifications and extensions introduced here, including the AI-related amplification mechanisms and scenario analyses, are the contributions of the present author. Due to intellectual property considerations and to respect the original author, and following standard academic practice for model modifications, the executable code of the modified model cannot be publicly released.

Therefore, the results after all modifications are illustrated and documented using the original diagrams presented in subsection 3.1, which demonstrate the impact of the AI-related modifications. However, full model specifications, network structures, algorithmic definitions, parameter configurations, and simulation protocols are provided

in textual form to ensure the reproducibility of the study. It is important to note that only a minimal portion of the original model was used, specifically the general concept of nodes connected by links, while all AI-related modifications and the direct risk evaluation mechanism were developed independently by the present author. These enhancements extend the model's capabilities, allowing it to be used not only as a conceptual tool but also as a practical framework for comparative risk analysis.

It should be noted that no formal mathematical equations beyond those directly represented in the code portions (Table 1) have been introduced in this work. All aspects of the model, including initialization, updating rules, stopping condition, and risk computations, reflect the actual implementation in the modified model. This textual and conceptual specification ensures that the study remains fully reproducible without the need to release the executable code. In order to achieve further clarity and formal precision, the author specifies the model and simulation logic, as follows:

- *initialization* – in this case all node risk intensities are set to their baseline values.
- *update rules* – AI-related amplification is applied once per scenario configuration to avoid exponential growth.
- *stopping condition* – actually each simulation runs proceeds for a fixed number of steps as defined in the baseline model.
- *randomness* – the model operates fully deterministically without any stochastic components or random seeds.

The AI mechanism applied in the simulation model operates as an amplification of the influence of internodes by modifying the weights of links associated with AI-related nodes. Since the reference model does not include explicit link weights, all links are conditionally assumed to have a unit baseline weight, serving as the reference for amplification. Formally, this process can be expressed as a transformation of link weights: $w_{ij_modified} = w_{ij_reference} * \alpha$, where $w_{ij_reference}$ represents the conceptual baseline weight of the link between nodes i and j , $w_{ij_modified}$ defines the weight after applying the AI amplification factor α , and α is applied once per scenario configuration. Moreover, α can vary across scenarios to simulate different levels of AI influence.

For example, $\alpha = 0$ represents maximum protection (no AI amplification), $\alpha = 1$ corresponds to no change from the baseline weights, and $\alpha > 1$ means increasing levels of AI amplification. For each node the risk intensity (i) is defined conceptually as $R_i = R_{i_reference} * \alpha_i$, where $R_{i_reference}$ represents the baseline risk of node i , and α_i is associated with AI-related effects for that node. This means that the normalized risk intensity of node i is then defined as $R_{i_norm} = 100 * R_i / \sum_j R_{j_max}$, where R_{j_max} is the sum of maximum risk intensities across all nodes in the network. It is important to note that α_i is used once per scenario configuration rather than at each simulation step (tick). By this solution the author aims to prevent unrealistic exponential escalation of weights, ensuring that the risk propagation remains consistent with the intended scenario parameters.

3.1. Assessment and analysis of the simulation results

The simulation was completed in ten scenarios for different *ai-weights*. Fig. 5 shows the dependence of normalized risk intensity across morphic chain types for *ai-weight* = 0, corresponding to maximum cyber protection, and for *ai-weight* = 4.5, corresponding

to maximum adverse AI effects and risk intensity. Table 2 includes the simulation results obtained in all ten scenarios. The normalized risk intensity (R_{i_norm}) is expressed in percentages, based on the conditional assumption that it represents the potential level of risk.

In the “maximum protection” scenario ($ai_weight = 0$) the risk intensity does not fall to zero because the baseline risk values of the nodes are strictly positive and the network contains residual interconnections. This means that even without AI amplification, each node keeps its inherent baseline risk, and the propagation of influence through the weighted network maintains a risk level that is not equal to 0. Consequently, the normalized risk intensity in this scenario is approximately equal to the low value of 25%, reflecting the cumulative contribution of the baseline risks and the underlying network structure.

The morphic chain type in the plot aims to maintain consistency with the shortest-path representation in the reference model, although its value is equal to 1 in all scenarios and does not affect the simulation results. Actually, the shortest-path diagram visualizes the distribution of path lengths in the network, as in the original and reference models, and is used only for structural comparative analysis. Although it does not provide information on risk intensity, it is suitable for illustrating consistency in the network topology.

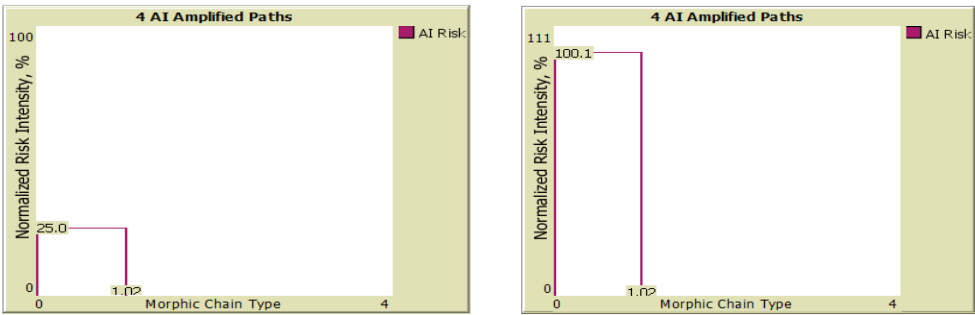


Fig. 5. Dependence of normalized risk intensity across morphic chain types for $ai_weight = 0$, corresponding to maximum cyber protection, and for $ai_weight = 4.5$, corresponding to maximum adverse AI effects and risk intensity.

Table 2.

<i>AI weight (α)</i>	<i>Normalized Risk Intensity (R_{i_norm}), %</i>
0	25
0.5	26
1	29
1.5	34
2	41
2.5	50
3	61
3.5	74
4	89
4.5	100

4. CONCLUSION

The comprehensive conclusions from the simulation research, based on the reliable results, demonstrate the dual role of AI technologies in the network. Their capabilities for ensuring cyber protection can contribute to reducing potential risks of cyberattacks. Besides, the modified simulation model by the author is adapted to a conditional measure of the adverse effects of AI technologies, by assessing the normalized risk intensity.

Besides, an important advantage of the methodology presented in this study is that it provides a clear and detailed framework for modeling AI-related amplification of cyber risks. This allows researchers with programming expertise and a background in cyber security to understand the logic of the model and, if desired, to develop advanced models analogous to the one presented by the author, without the need to access the executable code. An additional advantage of the methodology presented is its flexibility, because the fully described concept and mechanisms of this study allow the implementation of the model in other programming environments or software platforms, facilitating adaptation and further development without relying on NetLogo.

These advantages of the study could provide a foundation for future exploration of emerging trends in the cybersecurity area. Specific AI technologies, such as machine-learning-based intrusion detection systems, automated threat intelligence platforms, and generative AI tools for anomaly detection, can effectively contribute to the development of advanced cyber protection mechanisms. For example, generative technologies have the capability to analyze large volumes of data and identify patterns [13], making them applicable for cybersecurity purposes.

REFERENCES

- [1] *World Economic Forum*, The Global Risks Report 2023 (18th Edition Insight Report), Geneva, Switzerland, 2023, ISBN-13: 978-2-940631-36-0, pp. 9-10, Available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (Visited on 26.01.2026).
- [2] *World Economic Forum*, The Global Risks Report 2024 (19th Edition Insight Report), Geneva, Switzerland, 2024, ISBN: 978-2-940631-64-3, pp. 8-9, Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (Visited on 26.01.2026).
- [3] *World Economic Forum*, The Global Risks Report 2025 (20th Edition Insight Report), Geneva, Switzerland, 2025, ISBN: 978-2-940631-30-8, pp. 8-10, Available at: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf (Visited on 26.01.2026).
- [4] Gonçalves, C. P. S. *Cyber Threats to Global Governance*, 2012, Available at: http://modelingcommons.org/browse/one_model/3423#model_tabs_browse_info (Visited on 26.01.2026).
- [5] *World Economic Forum*, Global Risks 2012 (7th Edition Insight Report), Geneva, Copyright © 2012, ISBN: 92-95044-35-5, 978-92-95044-35-7, pp. 6
- [6] *World Economic Forum*, Global Risks 2015 (10th Edition Insight Report), Geneva, Copyright © 2015, pp. 4

- [7] Sapundzhi, F., Danev, K., Ivanova, A., Popstoilov, M., Georgiev, S. A performance comparison of shortest path algorithms in directed graphs. *14th International Scientific Conference TechSys 2025 - Engineering, Technologies and Systems*, vol. 100, no 1, 2025, ISSN 2673-4591, pp. 31, <https://doi.org/10.3390/engproc2025100031>
- [8] Martin, D. P., *Dynamic Shortest Path and Transitive Closure Algorithms: A Survey*, Computer Science, Cornell University, 2017, arXiv:1709.00553 [cs.DS], <https://doi.org/10.48550/arXiv.1709.00553>
- [9] Wilenski, U., NetLogo, Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL, 1999, Available at: <http://ccl.northwestern.edu/netlogo/> (Visited on 26.01.2026).
- [10] Soulé J., Jamont J., Occell M., Théron p., Traonouez L., Towards a Multi-Agent Simulation of Cyber-attackers and Cyber-defenders Battles, *Artificial Intelligence (cs. AI)*, arXiv:2506.04849 [cs.AI], 2025, <https://doi.org/10.48550/arXiv.2506.04849>
- [11] Jiang Y., Oo N., Meng Q., Lin L., Niyato D., Xiong Z., Lim H. W., Bikdar B., CyGATE: Game-Theoretic Cyber Attack-Defense Engine for Patch Strategy Optimization, *Cryptography and Security (cs.CR); Artificial Intelligence (cs.AI)*, arXiv:2508.00478 [cs.CR], 2025, <https://doi.org/10.48550/arXiv.2508.00478>
- [12] Landolt C. R., Würsch C., Meier R., Mermoud A., Jang-Jaccard J., Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications, *Multiagent Systems (cs.MA); Computer Science and Game Theory (cs.GT); Machine Learning (cs.LG)*, arXiv:2505.19837 [cs.MA], 2025, <https://doi.org/10.48550/arXiv.2505.19837>
- [13] Rashidov, A. Analysis and evaluation of satisfaction and preferences regarding the use of artificial intelligence in education. *International Journal on Information Technologies and Security*, vol.17, no.4, 2025, pp. 23-32, <https://doi.org/10.59035/STBI7753>

Information about author:

Assoc. Prof. Dr. Yoana A. Ivanova is a lecturer in the Department of Telecommunications at NBU; Professional area: 5.3. "Communication and computer equipment"; Area of scientific research: Communication and Information Systems and Technologies in Security.

Manuscript received on 26 January 2026