Human Factors in Cybersecurity, Vol. 127, 2024, 83–93
https://doi.org/10.54941/ahfe1004768

A Survey of Agent-Based Modeling for Cybersecurity

Arnstein Vestad and Bian Yang

Norwegian University of Science and Technology (NTNU), Trondheim/Gjøvik, Norway

ABSTRACT

Cybersecurity is a complex problem, and research on complex adaptive systems has been utilized in many research disciplines to understand complexity and emergent behavior. Agent-based modeling (ABM) has been identified as an essential tool for understanding how individual behavior from learning and adapting agents can result in unexpected results and give new insights. We have conducted a literature review on the use of ABMs in the cybersecurity domain, identified key issues and offer suggestions to improve the practice of ABM in the cybersecurity domain. We also discuss new possibilities for ABM-based research incorporating sensor-based systems and big data processing and a better understanding of human agents in cybersecurity.

Keywords: Cybersecurity, Agent-based modelling, Complex adaptive systems

INTRODUCTION

As the interconnectedness of systems, organizations, and society elevates cybersecurity challenges, traditional models fail to manage them effectively. Particularly, safeguarding complex adaptive systems where new threats constantly emerge remains demanding. Even managing the interactions of software installations within a medium-sized organization, considering their associated vulnerabilities in the software supply chain, becomes computationally rigorous. Adding organizational security procedures, continually adapting strategies from cyber-attackers, and increasing third-party dependencies to cloud services further underlines the complexity of organizational cybersecurity.

To address this complexity, researchers have proposed studying these systems through the lens of complex adaptive systems (CAS), which denote dynamically interacting and adaptable agents that impact the system as a whole, inducing emergent behavior (Carmichael and Hadžikadić, 2019). Agents in this context vary widely - from migratory birds to users on social media. Despite criticisms such as over-complexity and replicability issues, agent-based modeling (ABMs) has emerged as a potent tool for studying these systems. ABMs simulate agent interactions and assess their impact on the system, thus providing a bottom-up modeling approach.

This paper explores the application of ABMs in cybersecurity by reviewing existing applications and identifying improvement areas. Our analysis describes the current usage of ABMs on cybersecurity problems and identifies potential challenges and best practices. We support the review findings with insights from other areas where ABMs have been used successfully to formulate guidelines for ABM development in cybersecurity. The objective is to provide an overview of ABM's role in cybersecurity, underlining key issues, pitfalls, and potential research avenues.

For clarity, we first introduce the context of CAS and ABMs, then outline the literature survey's methodology that underpins study selection. Subsequent sections discuss key findings and trends from the survey. We delve into reasons for opting for ABMs, high-level model-building approaches, and widely-used tools and software specific to ABM in cybersecurity. We conclude by discussing how humans are modelled in ABMs, as well as challenges in model validation.

BACKGROUND

Complex adaptive systems (CAS) theory, characterized by emergence, self-organization, continuous adaptation, and non-linearity, is influential in various fields such as ecology, biology, and, more recently, in cybersecurity (Uluhan and Aydin, 2014).

Agent-based modeling has become a prominent tool for reasoning about such systems in a variety of fields, including the field of ecological systems studying ecosystems, survival, animal behavior strategies, and tradeoffs (An *et al.*, 2021) in the field of political science to model political strategy, elections, government formations, and market structures (de Marchi and Page, 2014), in the economy, to study markets, firm dynamics, stock prices, etc. (Farmer and Foley, 2009) and in the field of transport and energy transition, for example, to analyze the transition to electric vehicles (Mehdizadeh, Nordfjaern and Klöckner, 2022).

Various types of modeling and simulation have previously been suggested for use in cybersecurity, ranging from simulations for risk analysis, attack simulators simulating the exploitation of vulnerabilities in interconnected systems using graph theory, simulations to conduct training and cybersecurity exercises or to understand the effect of human cybersecurity actions (Kavak *et al.*, 2021). ABMs offer a 'bottom-up' modeling approach by identifying agents, analyzing their behaviors and interactions, fostering a deeper understanding of their impact on the system, for example impacts of alterations in security and regulatory policies (Norman and Koehler, 2017), and managing cognitive limitations of human agents (Renaud and Mackenzie, 2013).

An 'agent' in ABMs exhibits autonomous behavior, interacts with other agents or their environment, and may have diverse or conflicting goals. They can adapt their behavior based on their interactions. The richness in the construction and initial parameters of agents results in a variety of possible questions that can be modeled or simulated, introducing new ways to understand cybersecurity complexity. It also enables scaling model complexity ranging from simple toy models to advanced models built on empirically grounded data. However, ABMs face criticism concerning validation. Studies reveal the absence of model validation and discussions on agent interaction topology (Mehdizadeh, Nordfjaern and Klöckner, 2022). The lack of empirical data calibration, validation criteria, and theoretical models may lead to distrust in ABM reliability for complexity issues in cybersecurity. This paper give some suggestions to tackle these challenges in the ensuing discussion.

METHODOLOGY

The main objective of this survey is to present the current status and practice of ABMs in cybersecurity and to discuss methodological improvements and guidelines. In order to answer our research questions we conducted a literature review following the suggested steps of (Fink, 2020), including the steps of selecting research questions, selecting databases, choosing search terms, applying practical and methodological quality screening, and extracting and synthesizing the results. For the search, we decided to focus on the major information systems and computer science databases, including SpringerLink, IEEE, the AIS, and the ACM digital libraries. We established the following search terms:

```
("agent based" OR "agent-based") AND ("cybersecurity"
OR "computer security" OR ``information security)
```

We developed inclusion and inclusion criteria – the modelling/simulation must be in the area of cybersecurity, and the paper must describe the actual use of agent-based models. We chose not to set a specific timeframe but required that the included research should be from peer-reviewed conferences and journals. We exclude papers focusing on purposes other than simulations or only theoretical discussions.

The initial search identified a total of 938 papers, a screening of abstracts reduced this number down to 62. A further full reading of the papers and validation against the inclusion/exclusion criteria further reduced this to 34. In addition 5 papers were added as a result of snowballing (identifying new papers from the references in already included papers) or extra searches through Google Scholar and Scopus.

Table 1. Literature survey – sources and the number of included articles.

Database	Initial Search	Title and Abstract Screening	After Reading
SpringerLink	663	35	16
IEEE	569	18	11
AIS digital library	65	2	1
ACM Digital library	156	9	6
Snowball and additional searches	NA	NA	5
Total	1453	64	39

RESULTS

The 39 identified papers were reviewed, and information was extracted on their respective arguments for the use of ABMs for their specific model purposes, the problem domain addressed, their modeling approaches, and the software utilized to implement the model. With the exception of some sporadic earlier attempts, an uptake can be identified from 2012, with a peak in 2017.

Why Agent-Based Simulations in Cybersecurity?

Agent-based models (ABMs) are favored for their ability to simulate complex adaptive systems, especially in scenarios where traditional differential equation models are inadequate (Burns *et al.*, 2017), (Kotenko and Ulanov, 2007), (Zoto *et al.*, 2018). Unlike simpler models, ABMs effectively handle heterogeneity among agents and complex feedback loops, offering insights into non-linear patterns from micro-level interactions (Kiesling *et al.*, 2012). (Burns *et al.*, 2017) highlight that ABMs can model cybersecurity within organizations as complex systems, focusing on individual agent interactions and their cumulative impact on the system's overall state. (Bayir *et al.*, 2020) and (Wagner *et al.*, 2015) note that ABMs' "bottom-up" approach, starting from the micro-level, simplifies the simulation process, facilitating the study of emergent behavior without requiring comprehensive knowledge of global system interdependencies.

Additionally, ABMs are valued for their accessibility and ease of communication. They are relatively simple to construct, comprehend, and discuss, as pointed out by (Bayir *et al.*, 2020) and (Burns *et al.*, 2017). User-friendly interfaces in some ABM software further simplify model creation and enable engagement with non-technical stakeholders (Wagner *et al.*, 2015). (Burns *et al.*, 2017) and (Qureshi and Ahmad, 2022) emphasize ABMs' utility in training and instruction through visualization and graphical interfaces, making complex simulations more relatable.

Finally, ABMs are instrumental in exploring cybersecurity issues tied to human behavior and organizational policies. They incorporate individual differences, empirical data, and psychological aspects, thereby providing a nuanced understanding of security incidents in organizations (Rausch *et al.*, 2018), (Novak, Christopher *et al.*, 2017). These models also consider social and cognitive factors, offering a valuable supplement to empirical studies and traditional game-theoretic models in examining human behavior.

Applications of ABMs in Cybersecurity

The use of ABMs in cybersecurity also covers a wide range of applications both in the technological and human/organizational domains, and our analysis identified 7 subject areas:

- **Spread of malware:** ABMs model the spread of malware, where the agents can be malicious software and computing nodes (Batista, del Rey and Queiruga-Dios, 2020), in different network topologies (Wagner *et al.*, 2016), response strategies (Ishinishi, Tanuma and Deguchi, 2007), noisy or more covert infections (Lee-Urban *et al.*, 2016), in mobile tactical networks (Morris-King and Cam, 2015) or human responses (Chumachenko and Yakovlev, 2019)

- **Social networks** – ABMs analyze social media dynamics, including the spread of fake news by bots (Blane, Moffitt and Carley, 2021) and the impact of social media policy changes (Onuchowska and Berndt, 2019).
- **Human and organizational issues**: Studies focus on various aspects like sanctions and motivation (Burns *et al.*, 2017), compliance audit strategies (Casey *et al.*, 2016), user fatigue (Rausch *et al.*, 2018), password strategies (Novak, Christopher *et al.*, 2017)(Kothari *et al.*, 2015)(Renaud and Mackenzie, 2013), trust in incident management (Cunningham and Roque, 2017), learning from interactions (Diamadi and Fischer, 2001), inter-organizational trust (Deljoo *et al.*, 2018), cyber situational awareness (Dobson and Carley, 2018), and the impact of company characteristics on security incidents (Shin *et al.*, 2022).
- **Risk analysis and risk propagation:** Simulating accumulated incident costs (Ashiku and Dagli, 2020), (Bayir *et al.*, 2020), systemic risk in system-of-systems (Tundis *et al.*, 2017) and in Cyber-Physical systems (Koutiva, Moraitis and Makropoulos, 2021).
- **Technological attack and defense strategies:** Research includes optimal defense strategies (Nochenson and Heimann, 2012)(Hofmeyr *et al.*, 2013), ICS systems defense (Fielder, Li and Hankin, 2016) (Abercrombie, Schlicher and Sheldon, 2014), software diversity (Chen, Cam and Xu, 2021), and blockchain in smart-grid networks (Qureshi and Ahmad, 2022) or cooperation in DDoS attack management (Kotenko, Konovalov and Shorov, 2010).
- **Policy evaluation:** Effects of network policies (Wagner *et al.*, 2015) application whitelisting (Norman and Koehler, 2017) organizational structures fraud detection(Grabis and Rasnacis, 2019), database access policies (Chiong and Dhakal, 2008).
- **Strategic Outcomes:** Investigating attack/defense strategies (Chapman *et al.*, 2014) and architectural choices (Puchaty and DeLaurentis, 2011).

Several of the reviewed papers highlighted the suitability of using ABMs for investigating policy or strategy choices in system-of-systems or in a socio-technical perspective where simulations may cross between technical networks and organizational or human issues such as organizational or individual performance, cognitive loads, trust evaluation or cooperation, illustrating how well-suited ABMs are for investigating socio-technical cybersecurity issues.

Tools

Agent based models in cybersecurity can be programmed both by using general purpose software, specialized agent based simulation software, specialized programming frameworks and with general purpose programming languages such as Python and Java. While simple ABMs can be built in Microsoft Excel and similar spreadsheets with macro support (C. M. Macal & North, 2005), the only general purpose software found was the use of

Matlab. About half of the models were built on dedicated ABM software: Netlogo, with its turtle/patch based logic, sometimes supported with additional logic in python, Repast Simphony, an open source interactive java based modeling toolkit and the commercial software Anylogic that support different types of simulations including ABMs.

MESA, a framework for python, or JADE (JAVA Agent DEvelopment Framework) a multi-agent framework for Java as well as OMNet++, a toolkit for network simulations were used by several of the models, while Python and Java were the languages chosen for models built from scratch. 3 of the papers did not describe their software implementation, which may constitute a problem for reproducibility.

DISCUSSION

Based on the findings of the literature survey we will focus the discussion on two important areas – the representation of humans in cybersecurity ABMs, as well as the validation of models.

Model Building and the Human Element

When modeling human agents, the modeler must decide the level of decision logic necessary for answering the research question. Full human-level artificial intelligence is rarely necessary for modeling the type of aggregated results that is usually the intended outcome of ABMs, but the reviewed literature gives some suggestions towards factors to consider, such as bounded rationality, stress, and cognitive limitations such as the ability to remember passwords and emotions. Modeling and predicting human behavior is by nature complex and should prove fertile ground for ABM-based models, however, humans modeled so far in cybersecurity are frequently simplistic representations, sometimes reduced to simple rates such as "user gullibility" (Rausch *et al.*, 2018) or responding to generic representations of security awareness trainings (Norman and Koehler, 2017). It seems clear that modeling of human behavior in cybersecurity is lacking in theoretic foundations, a finding echoed by (Kavak *et al.*, 2021), and cybersecurity modeling would do well in learning from other fields, such as psychology and sociology to base human models on well-founded mental models. Some examples can be found in (Kennedy, 2012) that give an overview of possible theories and typical challenges when modeling human behavior, while (Schlüter *et al.*, 2017) illustrate how different theories of human decision making might be used in ABMs, such as theory of planned behavior, descriptive norm or reinforcement learning. The rich literature on human motivation, personality, and cognitive decision processes gives fertile ground to build logic for simulations that can provide novel results from discovering emergent behaviors.

Simulation Validation

Previous studies have raised concerns about the validation of ABM research (Mehdizadeh, Nordfjaern and Klöckner, 2022), a finding we echo in our analysis. Few of the reviewed papers discuss empirical calibration and validation, a concern for the validity of the suggested models. Of 36 surveyed papers, 27 papers give limited to no description of how the simulations was validated, a serious methodological weakness. Of those that discuss validation, several only discuss face validation and validation with subject matter experts.

Model validation should account for three main steps – 1 – verification of the correctness of the implementation of the model, 2 – validation against external criteria, for example empirical data, expert knowledge or other models, and 3 – sensitivity analysis – verifying the robustness and sensitivity of the model to changes in input parameters (Cooley and Solano, 2011). Several techniques may be utilized to verify the simulations, from simple expert validation, aided by the ABMs animation/visualization functionality, to validating against empirical data. While empirical data in the cybersecurity domain has traditionally been a challenge due to confidentiality requirements, regulations requiring mandatory reporting of incidents, such as HIPAA and the GDRP may give rise to better datasets to validate simulations. General guidelines for model verification and validation, such as (Sargent, 2010), should be utilized to improve the quality of ABM cybersecurity models and simulations.

New Opportunities for ABMs in Cybersecurity

The emergence of sensor-based systems, including IoT and mobile devices, and big data solutions capable of processing vast streams of data, could refocus attention on ABMs. Integrating these technologies with ABM research may enhance understanding of individual agent behaviors, thereby improving the empirical foundation of these models. Additionally, advancements in computational power are enabling more intricate ABM simulations. These simulations can explore complex interactions across different model levels and types, such as individuals and organizations, organizations and ecosystems, and technological and organizational levels. This approach could yield new insights into the societal impacts of cyber-attacks, underpinned by detailed technological attack graphs and simulations of critical IT/OT infrastructures

Furthermore, ABMs' visual and incremental nature, coupled with their bottom-up modeling approach, positions them well for enhancing cybersecurity awareness in education and public domains. They can act as "boundary objects" (Star, 1989), bridging the gap in understanding and facilitating improved communication between technical security personnel and non-technical stakeholders.

CONCLUSION

Through our survey we have identified the use of ABMs to investigate a diverse set of problems in the cybersecurity domain, but also identified some key challenges that need to be addressed for ABMs to have a larger role in the understanding of complex cybersecurity challenges. We have also given suggestions that can serve as a guideline to improve the practice of agent-based modelling in cybersecurity and identified some possible avenues of further ABM-based research, including suggestions on how to improve the modelling of human actors. By following well-established and robust practices for model building and validation, agent-based modelling can remain an important tool in cybersecurity.

ACKNOWLEDGMENT

This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105.

REFERENCES

Abercrombie, R. K., Schlicher, B. G. and Sheldon, F. T. (2014) 'Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation', in 47. Hawaii Int. Conf. on System Sciences. At: https://doi.org/10.1109/HICSS.2014.255

An, L. et al. (2021) 'Challenges, tasks, and opportunities in modeling agent-based complex systems', Ecological Modelling. doi: https://doi.org/10.1016/j.ecolmodel.2021.109685.

Ashiku, L. and Dagli, C. (2020) 'Agent Based Cybersecurity Model for Business Entity Risk Assessment', in 2020 IEEE International Symposium on Systems Engineering (ISSE). doi: https://doi.org/10.1109/ISSE49799.2020.9272234.

Axtell, R. (2000) 'Why Agents? On the Varied Motivations for Agent Computing in the Social Sciences'.

Batista, F. K., del Rey, A. M. and Queiruga-Dios, A. (2020) 'A Review of SEIR-D Agent-Based Model', in E. Herrera-Viedma et al. (eds) Distributed Computing and Artificial Intelligence, 16th Int. Conf. doi: https://doi.org/10.1007/978-3-030-23946-6_15.

Bayir, B. et al. (2020) 'Company Security Assesment with Agent Based Simulation', in 2020 Innovations in Intelligent Systems and Applications Conference (ASYU). Available at: https://doi.org/10.1109/ASYU50717.2020.9259865.

Blane, J. T., Moffitt, J. D. and Carley, K. M. (2021) 'Simulating Social-Cyber Maneuvers to Deter Disinformation Campaigns', in R. Thomson et al. (eds) Social, Cultural, and Behavioral Modeling. Available at: https://doi.org/10.1007/978-3-030-80387-2_15.

Burns, A. J. et al. (2017) 'Organizational information security as a complex adaptive system: insights from three agent-based models', Information Systems Frontiers, 19(3), pp. 509–524. Available at: https://doi.org/10.1007/s10796-015-9608-8.

Carmichael, T. and Hadžikadić, M. (2019) 'The Fundamentals of Complex Adaptive Systems', in T. Carmichael, A. J. Collins, and M. Hadžikadić (eds) Complex Adaptive Systems: Views from the Physical, Natural, and Social Sciences. Available at: https://doi.org/10.1007/978-3-030-20309-2_1.

Casey, W. et al. (2016) 'Compliance signaling games: toward modeling the deterrence of insider threats', Computational and Mathematical Organization Theory, 22(3), pp. 318–349. Available at: https://doi.org/10.1007/s10588-016-9221-5.

Chapman, M. et al. (2014) 'Playing Hide-and-Seek: An Abstract Game for Cyber Security', in Proceedings of the 1st International Workshop on Agents and Cyber-Security. New York, NY, USA - Available at: https://doi.org/10.1145/2602945.2602946.

Chen, H., Cam, H. and Xu, S. (2021) 'Quantifying Cybersecurity Effectiveness of Dynamic Network Diversity', IEEE Transactions on Dependable and Secure Computing, pp. 1–1. Available at: https://doi.org/10.1109/TDSC.2021.3107514.

Chiong, R. and Dhakal, S. (2008) 'Modelling Database Security through Agent-Based Simulation', in 2008 Second Asia International Conference on Modelling & Simulation (AMS). Available at: https://doi.org/10.1109/AMS.2008.164.

Chumachenko, D. and Yakovlev, S. (2019) 'On Intelligent Agent-Based Simulation of Network Worms Propagation', in 2019 IEEE 15th Int. Conf. on the Experience of Designing and Appl. of CAD Systems. https://doi.org/10.1109/CADSM.2019.8779342

Cooley, P. and Solano, E. (2011) 'Agent-Beased Model (ABM) Validation Considerations' https://www.rti.org/sites/default/files/resources/simul_2011_7_10_50045.pdf.

Cunningham, C. and Roque, A. (2017) 'Adapting an agent-based model of socio-technical systems to analyze security failures', in 2017 IEEE International Symposium on Technologies for Homeland Security. doi: https://doi.org/10.1109/THS.2017.7943457.

Deljoo, A. et al. (2018) 'Social Computational Trust Model (SCTM): A Framework to Facilitate Selection of Partners', in 2018 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS). Available at: https://doi.org/10.1109/INDIS.2018.00008.

de Marchi, S. and Page, S. E. (2014) 'Agent-Based Models', Annual Review of Political Science. At: https://doi.org/10.1146/annurev-polisci-080812-191558.

Diamadi, Z. and Fischer, M. J. (2001) 'A simple game for the study of trust in distributed systems', Wuhan University Journal of Natural Sciences, 6(1), pp. 72–82. Available at: https://doi.org/10.1007/BF03160228.

Dobson, G. B. and Carley, K. M. (2018) 'A Computational Model of Cyber Situational Awareness', in R. Thomson et al. (eds) Social, Cultural, and Behavioral Modeling. doi: https://doi.org/10.1007/978-3-319-93372-6_43.

Farmer, J. D. and Foley, D. (2009) 'The economy needs agent-based modelling', Nature, 460(7256), pp. 685–686. Available at: https://doi.org/10.1038/460685a.

Fielder, A., Li, T. and Hankin, C. (2016) 'Modelling Cost-Effectiveness of Defenses in Industrial Control Systems', in A. Skavhaug, J. Guiochet, and F. Bitsch (eds) Computer Safety, Reliability, and Security. doi: https://doi.org/10.1007/978-3-319-45477-1_15.

Fink, A. (2020) Conducting research literature reviews: from the internet to paper. Fifth edition. Los Angeles: Sage.

Grabis, J. and Rasnacis, A. (2019) 'Simulation Based Evaluation and Tuning of Distributed Fraud Detection Algorithm', in Proceedings of the Winter Simulation Conference. IEEE Press (WSC '19), pp. 786–796.

Heckbert, S., Baynes, T. and Reeson, A. (2010) 'Agent-based modeling in ecological economics', Annals of the New York Academy of Sciences, 1185(1), pp. 39–53. Available at: https://doi.org/10.1111/j.1749-6632.2009.05286.x.

Hofmeyr, S. et al. (2013) 'Modeling Internet-Scale Policies for Cleaning up Malware', in B. Schneier (ed.) Economics of Information Security and Privacy III. New York, NY. Available at: https://doi.org/10.1007/978-1-4614-1981-5_7.

Ishinishi, M., Tanuma, H. and Deguchi, H. (2007) 'A Study on Countermeasures against Computer Virus Propagation Using an Agent-based Approach', in T. Terano et al. (eds) Agent-Based Approaches in Economic and Social Complex Systems IV. Available at: https://doi.org/10.1007/978-4-431-71307-4_10.

Kavak, H. et al. (2021) 'Simulation for cybersecurity: state of the art and future directions', Journal of Cybersecurity,. Available at: https://doi.org/10.1093/cybsec/tyab005.

Kennedy, W. (2012) 'Modelling Human Behaviour in Agent-Based Models', in, pp. 167–179. Available at: https://doi.org/10.1007/978-90-481-8927-4_9.

Kiesling, E. et al. (2012) 'Agent-based simulation of innovation diffusion: a review', Central European Journal of Operations Research, 20(2), pp. 183–230. Available at: https://doi.org/10.1007/s10100-011-0210-y.

Kotenko, I., Konovalov, A. and Shorov, A. (2010) 'Simulation of Botnets: Agent-Based Approach', in M. Essaaidi, M. Malgeri, and C. Badica (eds) Intelligent Distributed Computing IV. Available at: https://doi.org/10.1007/978-3-642-15211-5_26.

Kotenko, I. and Ulanov, A. (2007) 'Multi-agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks', in V. Gorodetsky et al. (eds) Autonomous Intelligent Systems: Multi-Agents and Data Mining. Available at: https://doi.org/10.1007/978-3-540-72839-9_18.

Kothari, V. et al. (2015) 'Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling', in Proc. 2015 Symp. and Bootcamp on the Science of Security. doi: https://doi.org/10.1145/2746194.2746207.

Koutiva, I., Moraitis, G. and Makropoulos, C. (2021) 'An Agent-Based Modelling approach to assess risk in Cyber-Physical Systems (CPS)', Available at: https://doi.org/10.30955/gnc2021.00194.

Lee-Urban, S. et al. (2016) 'Two Complementary Network Modeling and Simulation Approaches to Aid in Understanding Advanced Cyber Threats', in D. Nicholson (ed.) doi: https://doi.org/10.1007/978-3-319-41932-9_33.

Macal, C. and North, M. (2009) 'Agent-based modeling and simulation', in. Proc. of the 2009 Winter Simulation Conference. At: https://doi.org/10.1109/WSC.2009.5429318.

Mehdizadeh, M., Nordfjaern, T. and Klöckner, C. A. (2022) 'A systematic review of the agent-based modelling/simulation paradigm in mobility transition', Technological Forecasting and Social Change. At: https://doi.org/10.1016/j.techfore.2022.122011.

Morris-King, J. and Cam, H. (2015) 'Ecology-inspired cyber risk model for propagation of vulnerability exploitation in tactical edge', in MILCOM 2015. Available at: https://doi.org/10.1109/MILCOM.2015.7357465.

Nochenson, A. and Heimann, C. F. L. (2012) 'Simulation and Game-Theoretic Analysis of an Attacker-Defender Game', in J. Grossklags and J. Walrand (eds) Decision and Game Theory for Security. doi: https://doi.org/10.1007/978-3-642-34266-0_8.

Norman, M. D. and Koehler, M. T. K. (2017) 'Cyber Defense as a Complex Adaptive System: A Model-Based Approach to Strategic Policy Design', in Proceedings of the 2017 International Conference of The Computational Social Science Society of the Americas. Available at: https://doi.org/10.1145/3145574.3145595.

Novak, Christopher et al. (2017) 'Modeling Aggregate Security with User Agents that Employ Password Memorization Techniques', Thirteenth Symp. on Usable Privacy and Security (SOUPS 2017). At: https://www.usenix.org/conference/soups2017/workshop-program/way2017/novak

Onuchowska, A. and Berndt, D. J. (2019) 'Using Agent-Based Modelling to Address Malicious Behavior on Social Media', ICIS 2019 Proceedings [Preprint]. Available at: https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/24.

Puchaty, E. M. and DeLaurentis, D. A. (2011) 'A performance study of UAV-based sensor networks under cyber attack', in 2011 6th International Conference on System of Systems Engineering. Available at: https://doi.org/10.1109/SYSOSE.2011.5966600.

Qureshi, A. and Ahmad, K. (2022) 'Agents and Secure Contracts in Cyber-Physical Systems: A Simulation', in K. Arai (ed.) Proceedings of the Future Technologies Conference (FTC) 2021, Vol. 1. At: https://doi.org/10.1007/978-3-030-89906-6_36.

Rausch, M. et al. (2018) 'Modeling Humans: A General Agent Model for the Evaluation of Security', in A. McIver and A. Horvath (eds) Quantitative Evaluation of Systems. Available at: https://doi.org/10.1007/978-3-319-99154-2_23.

Renaud, K. and Mackenzie, L. (2013) 'SimPass: Quantifying the Impact of Password Behaviours and Policy Directives on an Organisation's Systems', Journal of Artificial Societies and Social Simulation, 16(3), p. 3. doi: https://doi.org/10.18564/jasss.2181.

Sargent, R. G. (2010) 'Verification and validation of simulation models', in Proceedings of the 2010 Winter Simulation Conference. Proceedings of the 2010 Winter Simulation Conference, pp. 166–183. Available at: https://doi.org/10.1109/WSC.2010.5679166.

Schlüter, M. et al. (2017) 'A framework for mapping and comparing behavioural theories in models of social-ecological systems', Ecological Economics, 131, pp. 21–35. Available at: https://doi.org/10.1016/j.ecolecon.2016.08.008.

Shin, J. et al. (2022) 'OSIRIS: Organization Simulation in Response to Intrusion Strategies', in R. Thomson, C. Dancy, and A. Pyke (eds) Social, Cultural, and Behavioral Modeling. doi: https://doi.org/10.1007/978-3-031-17114-7_13.

Star, S. L. (1989) 'Chapter 2 - The Structure of Ill-Structured Solutions: Boundary Objects and Heterogeneous Distributed Problem Solving', https://doi.org/10.1016/B978-1-55860-092-8.50006-X.

Tundis, A. et al. (2017) 'Systemic Risk Modeling and Evaluation through Simulation and Bayesian Networks', in Proc. 12th International Conference on Availability, Reliability and Security. New York, NY, USA. doi: https://doi.org/10.1145/3098954.3098993.

Uluhan, E. and Aydin, M. N. (2014) 'Complex Adaptive Systems Theory in the Context of Business Process Management', in C. Zehbold (ed.) S-BPM ONE - Application Studies and Work in Progress. Available at: https://doi.org/10.1007/978-3-319-06191-7_10.

Wagner, N. et al. (2015) 'Agent-based simulation for assessing network security risk due to unauthorized hardware', in Proceedings of the Symposium on Agent-Directed Simulation.

Wagner, N. et al. (2016) 'Towards automated cyber decision support: A case study on network segmentation for security', in 2016 IEEE Symposium Series on Computational Intelligence (SSCI). Available at: https://doi.org/10.1109/SSCI.2016.7849908.

Zoto, E. et al. (2018) 'A Pilot Study in Cyber Security Education Using CyberAIMs: A Simulation-Based Experiment', in L. Drevin and M. Theocharidou (eds) Information Security Education – Towards a Cybersecure Society. At: https://doi.org/10.1007/978-3-319-99734-6_4.