Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 106, Issue 18, March/April 2019, Pages 65–75
https://doi.org/10.7250/csimq.2019-18.04

A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education

Erjon Zoto*, Mazaher Kianpour, Stewart James Kowalski, and Edgar Alonso Lopez-Rojas

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway

erjon.zoto@ntnu.no, mazaher.kianpour@ntnu.no, stewart.kowalski@ntnu.no, edgar.lopez@ntnu.no

Abstract. Cybersecurity decisions are made across a range of social, technical, economic, regulatory and political domains. There is a gap between what companies and institutions plan to do while developing their internal IS-related policies and what should be done according to a multi-stakeholder system perspective in this area. Our task as researchers is to bridge this gap by offering potential solutions. The aim of our work is to promote the usage of the socio-technical systems approach to support the emerging role of systems thinking in cybersecurity education, using simulation as a supporting tool for learning. Meanwhile, new trends in cybersecurity curricula suggest an important shift toward new thinking approaches such as adversarial and systems thinking. We explored individuals' adversarial and systems thinking skills in an open agent-based simulated environment and subsequently assessed the impact based on a participant survey. We discuss these results and point to directions for further investigation. The second contribution of the article is the provision of a tool for developing target users' skills in making quantitative risk decisions and giving them a deeper understanding of the importance and use of key indices in the cyber risk management process.

Keywords: Socio-technical Systems, Information Security, Systems Thinking, Adversarial Modeling, Agent-based Simulation, Risk Quantification.

1 Introduction

We hardly ever pass any day without hearing of new cybersecurity incidents affecting different stakeholders in society such as individuals, organizations, and national and international entities. With all these vulnerable systems and threat actors out there, organizations today are in a constant race to defend adequately against potential cyber-attackers through technical or social means. A properly educated and aware staff has been identified as one of the most cost-effective means to keep organizations ahead in the race [1].

* Corresponding author

© 2019 Erjon Zoto et al. This is an open access article licensed under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0).

Reference: E. Zoto, M. Kianpour, S. J. Kowalski, and E. A. Lopez-Rojas, "A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 18, pp. 65–75, 2019. Available: https://doi.org/10.7250/csimq.2019-18.04

Additional information. Author ORCID iD: E. Zoto: https://orcid.org/0000-0001-9231-5437, S. J. Kowalski: https://orcid.org/0000-0003-3601-8387, E. A. Lopez-Rojas: https://orcid.org/0000-0002-9158-3488. PII S225599221900106X. Received: 30 November 2018. Accepted: 14 March 2019. Available online: 30 April 2019.

In order to improve the cybersecurity education of the Information Technology (IT) staff, the Joint Task Force on Cybersecurity Education (JTF), a worldwide research group, was established to develop comprehensive curricular guidance in cybersecurity education. In 2017 JTF produced a new curricular volume that focused on new thinking processes, namely adversarial and systems thinking [2].

Lack of adversarial thinking – a process that considers the potential actions of the opposing force working against the desired result – in defenders leads to misplaced ideas of cybersecurity resilience and preparedness. According to systems thinking – a process that considers the interplay between social and technical constraints to enable assured operations – system behavior results from the effects of reinforced processes stemming from environments[1].

The aim of our research is to use a socio-technical systems (STS) approach to model and build a simulation-based teaching tool in adversarial and systems thinking, in order to raise the awareness of students and practitioners, in the ICT ecosystem, towards cybersecurity. A socio-technical approach enables us to systematically identify, describe, and study the more obscure, non-linear effects of multiple, dynamically shifting interactions among large collections of socio-technical system components [3]. Moreover, we employed a quantitative technique to estimate some of the key variables of information security risks to present a stronger case for training risk quantification and enhancement of cyber risk perception, based on information security economic principles. We know that cybersecurity risk is an inherently complex concept and is influenced by numerous socio-technical elements. However, in this article we focus on how investment in cybersecurity can mitigate the potential percentage of loss to a specific asset if an attack has occurred.

The ongoing modeling work is based on a combination of theoretical models [4] and data from real-world cases about cyber-attacks reported in the news[2]. In the simulation case, we present a scenario where attackers, having diversity in skills and motivations, try to break into different objectives; from states to individual customers/targets, while defenders use their skills and resources to stop and deter the attacks. The learning objectives of the simulator are: 1) indicate to users which of the different conditions are more relevant to making a cyber-attack and a cyber-defense effective, 2) quantify (defenders') losses due to cyber-attacks, 3) plan, formulate and make different risk quantification analyses for managing cases of cyber events, and 4) evaluate return on investment for information security spending.

This article has the following structure. In Section 2, we discuss the background and related works, while in Section 3, we describe the STS approach to designing the simulator. In particular, in Section 3.2, we explain the simulated method for cyber risk quantification. In Section 4, we show the results of the simulator being used by two target groups: the master students in the Information Security program and the Norwegian team in European Cybersecurity Challenge[3]. We discuss the risk quantification feature in Section 5. Finally, Section 6 summarizes this article and points out some directions for future work.

2 Background

Kowalski [5] argues that cybersecurity is a function of the interaction between various social and technical elements that characterize complex, adaptive socio-technical systems. A socio-technical system can be seen as being composed of two components: the social and the technical [6]. As Figure 1 shows, each of the components can be broken down into two sub-components. The social component has its cultural and structural sub-components, while the technical side has its own

[1] Socio-technical systems are subject to, and dependant on, their environment. The environment to some extent is being made up of a natural systems such as weather systems, geological systems, etc. and other socio-technical systems.

[2] https://thehackernews.com/2017/09/apt33-iranian-hackers.html

[3] https://www.enisa.europa.eu/events/european-cyber-security-challenge-ecsc-2018

machines and methods as sub-components. We have used the same approach when designing a simulator dealing with cybersecurity issues. In Figure 1 the arrows indicate mutual patterns of interchanges between the components, often unintended and unpredictable. That means a change in the machines used in the system will not only affect the methods used in the system but also its structure and culture.

Understanding and conceptualization of cybersecurity in a complex socio-technical system requires efficacious models and simulation tools, enabling enterprises to perform effective and secure system design and decision making by supporting accurate, shared mental models of the system dynamics. These tools should take into account the system's critical interrelating social and technical components so as to capture the system's uncertainties and complexity.

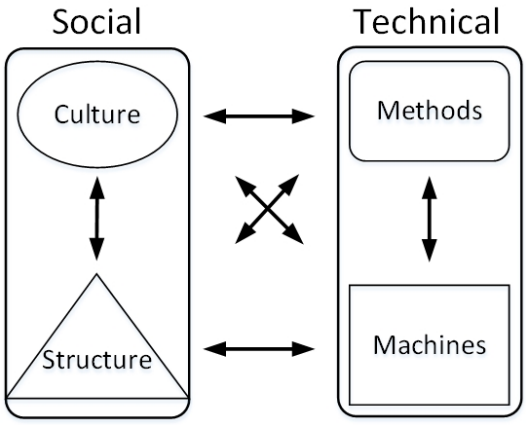


Figure 1. The typical socio-technical system

Pastor et al. [7] have done extensive research work on the available state-of-the-art simulation tools that can be used for the purpose of teaching and training. They suggest that such simulation tools should be designed to have a user-friendly interface and, at the same time, allow the user to obtain a deep understanding of the concepts.

We acknowledge that modeling and simulation create a good and efficient way to produce data that can be mapped to real cases of cyber events. The purpose of the modeling phase is to create a normalized view of the cybersecurity situation, while the simulation phase allows the imitation of typical attack activities against a specific infrastructure, with specific security controls in place, grouped in sets of possible scenarios. We built the tool in NetLogo [8], inspired by relevant work in the same area from Ben-Asher and Gonzalez [9] and a study prepared from the Ponemon Institute, [10] while developing their work further by introducing the STS approach within our tool.

Ben-Asher and Gonzalez came up with a simple cyberwar game that takes place in a network of n players. Each player has two main attributes, Power and Assets. Power represents the player's cybersecurity infrastructure, seen also as the investment in cybersecurity, while Assets entail the confidential information available for use.

The Ponemon Report showed the relationships between the time spent and compensation of today's cyber attackers and the way that organizations could thwart attacks. Some relevant findings were the average cost of $1,367 on a yearly basis for the tools that an attacker needs to execute his attacks and the average time spent against different target security infrastructures, ranging from 70 up to 209 hours.

Gordon and Loeb [11] proposed an economic model that determines the optimal amount to invest in protecting a given set of information from a single threat. The Single Loss Expectancy (SLE), the Annualized Rate of Occurrence (ARO) and the probability of a successful attack are three important parameters that they considered in their model. The model shows that optimal security spending does not essentially increase with the increasing vulnerability.

Tan [12] presented a quantitative method to cover more key variables in cyber risk quantification for tangible and intangible assets in firms. This method can be fine-tuned to meet the requirements of specific situations and specific industries. The analysis is often based on the facts that are typically important for different people such as security consultants, systems administrators and firms' upper management. This method is discussed in more detail in Section 3.2.

3 Implementation

3.1 Designing the Simulator with an STS Approach

We started designing the simulator by thinking that defense or attack actors in a potential cyberwar can be represented by their own socio-technical systems. Actors will have their own culture – defined by certain values, traditions, and laws, along with a certain structure – the actor's position in an organization or the whole society. They also have a certain level of access to the infrastructure already built (machines) and, depending on their former abilities and their will or cultural background, they can use the same or different available tools (methods) compared to their colleagues or potential opponents. Moreover, the type of infrastructure and tools in use should depend on the attitude of the actors or the structures above them regarding the amount of investments made while being part of the cyberwar.

Following the reasoning above, we defined three attributes that could explain the behavior and performance of the actors in the agent-based simulation tool. The attributes were Resources – the budget related to cyber activities, Skills – the level of training, literacy, and awareness of cyber events, and Motivation – the level of self-motivation and incentives behind potential actions in cyberspace in a certain time.

We used various sources of data for Resources, including [10], while we used the GCI Index, [13], for the Skills units. We did not make use of any relevant literature on Motivation, but we are willing to do so in the future stages.

Resources are most important when dealing with the technical component, spread equally between machines and methods for both attacks and defenses, and somewhat relevant when dealing with the structural sub-component, in the process of allocating funds to different strategies applied.

Skills are mostly related to the social component, almost equally spread between the cultural and structural sub-components, and somewhat relevant to the methods used. Motivation is generally related to the cultural background, but it can also be affected by the structural sub-component, depending on the direct links within the different levels of management. Motivation, depending on the incentives provided, can lead to the intentional or accidental misuse of machines. Both Skills and Motivation are slightly biased towards culture in the social component. Figure 2 depicts this type of relationships between each attribute and the STS sub-components, where attributes are located and weighed according to the reasoning above.

The first version of the simulator allowed the user to define the initial number of agents on each side of the battlefield and the initial value for each of the attributes for all agents on each side. The user is able to choose in a range of [1, 100] for the number of agents on each side, along with initial units of Resources and Motivation, and [1, 93] for the Skills attribute. Appendix A shows a screen-shot of the first version of the simulator's interface.

In that version, the simulator performed each run in a period of maximum 120 ticks. Each tick represents a fixed period of 3 days, mapping the minimum time required for an attacker to perform a successful attack [8], thus enabling it to predict the behavior of agents on both sides within a year. In addition, it allows a random attack agent to attack one or more random defense agents in each tick, but only if the former's combined product of attributes' units is at least a third of the combined product of attributes' units of the latter. That means that an attack agent should finish the attack in 3 ticks or less, otherwise it would quit the attack and target another opponent.

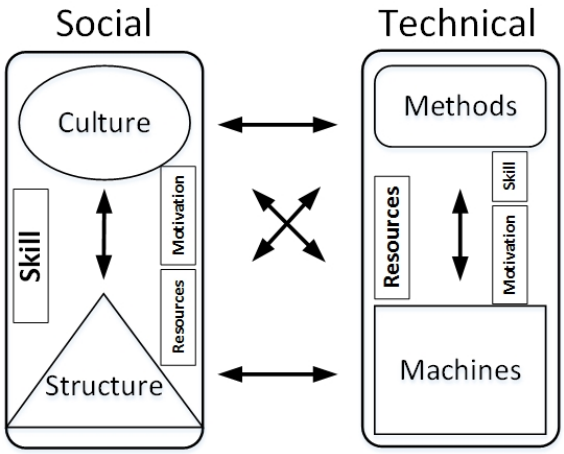


Figure 2. Attributes "produced" by the STS approach

If the attack was performed, the defense agent would lose some Resources units, based on the relative power that they had, compared to that of the attacker, taking in consideration the total amount of combined products between them, as shown from the expression (1) below. The successful attack agent would then gain the Resources units lost from the defense agent, while Skills units are also updated by increasing values on both sides, with the defense agent having a larger increase in terms of learning experience. Motivation is also updated on the attack agent's side, increasing the units by the value of the relative power below (1).

$$RelPower = Att(Res * Sk * Mot)/(Def(Res * Sk * Mot) + Att(Res * Sk * Mot)) \quad (1)$$

If the attack is avoided, only the Motivation units are updated on the defense agent side, by the same value of the relative power (1) above. Continuous successful attacks would decrease one of the defense agents' Resources units downwards until reaching zero. When this happens, the defense agent goes "offline", meaning he does not interact anymore with the other agents.

This agent-based simulation tool was named CyberAIMs, as an acronym for Cyber Agents' Interactive Modeling and Simulation. It shows that actors in cyberspace follow certain procedures and strategies according to their own aims, either as part of a higher entity or on an individual basis. CyberAIMs was built using NetLogo, which is a programmable modeling environment for simulating natural and social phenomena. NetLogo is particularly well suited for modeling complex systems which develop over time, with hundreds or thousands of agents, all operating independently.

3.2 Quantitative Risk Analysis

In the following subsections, we aim to introduce a simulation tool that allows users to develop their knowledge regarding the effectiveness of potential cybersecurity investments in mitigating the risk and damage from cyber attacks that may evantually occur. This feature will enable them to practice improving their reporting skills whenever they experience or predict potential losses from security incidents. We adopted a quantitative approach which assigns numeric values to the assets and the magnitude of loss arising from a successful attack. In spite of the fact that cybersecurity risk analysis is not limited to monetary loss assessment, in this article we reduce this complex concept down to a determinant factor in organizational policies. Several key variables are used to estimate the effectiveness of cybersecurity investments in an open socio-technical system, including a set of stakeholders and actors:

- **Exposure Factor (EF):** Percentage of loss of assets caused by cyber-attacks. This variable ranges from 0 to 100% depending on the countermeasures employed, attacker's location, potential rate of attack, etc.

- **Single Loss Expectancy (SLE):** The estimate of loss from a single occurrence of an attack (2).

$$SLE = AssetValue \times ExposureFactor \tag{2}$$

- **Annualized Rate of Occurrence (ARO):** The estimated frequency that an attack will occur during a year.
- **Annualized Loss Expectancy (ALE):** The expected monetary loss for a defender due to a risk incurred over one year (3).

$$ALE = SLE \times ARO \tag{3}$$

All of the above variables can be used to identify where security controls can be implemented and how their efficiency in deterrence, protection, detection, response and recovery from security threats and attacks can be measured.

3.3 Risk Quantification Using CyberAIMs

We implemented another version of CyberAIMs in order to show the importance of risk quantification and valuation of assets. As depicted in Appendix B, the user can choose the exposure factor and value of the assets in addition to the number of attackers and defenders in one round of the game. Asset value is a measure of creation, development, support and ownership values of an asset, the latter being categorized into tangible assets, such as network equipment, software, etc., as well as intangible assets, such as client confidence, experience, reputation, etc. The exposure factor, as discussed earlier, represents a measure of impact on the value of an asset due to an attack.

In this version of CyberAIMs, the corresponding values of Skills, Motivation and Resources attributes for both defense and attack agents are assigned randomly. Each step represents a 1-year period, where each defense agent may experience one or more security incidents, with a specific exposure factor and asset value accordingly. The simulation ends when all defense agents lose all of their resources and go offline, or after 10 steps (years). Users can modify the values of exposure factor and assets and run the simulation to see the results. This version will be an important part of future experiments; with students and industry representatives as relevant target groups in this process.

4 Experiments and Results

We have conducted four experiments using CyberAIMs to measure, from different perspectives, the impact that using the tool would have on the students' understanding of concepts related to adversarial and systems thinking, along with measuring the tool's level of usability and coverage from the cybersecurity professionals' perspective [14]. In this section, we will explain the results obtained from two of the experiments conducted, and we will continue by discussing our main findings in the next section.

Our first experiment using simulators was during the spring semester (2018) in a course entitled Socio-Technical Enabled Crime. This course is an elective course in a 2 years Master Program in Information Security, at the Norwegian University of Science and Technology (NTNU). The students attending the course, twelve in total, were asked to answer a pre-survey, followed, during the experiment, by a scenario of a recent real-world case of a cyber attack, and then complete the post-experiment survey. Eight students overall gave their feedback and used the simulator in order to provide their overall appreciation as related to learning adversarial and systems thinking.

Post-survey results indicate that three out of four students agreed on the importance of the simulation on developing their understanding of strategic management of information security. Two respondents stated that the simulation developed their risk management knowledge. Three respondents agreed that the simulation developed their understanding of real world cyber-scenarios. Regarding the main objective of this simulation-based experiment on learning outcomes, two

respondents agreed that the simulation did develop their understanding of systems thinking and, again, only two of them agreed on the statement about adversarial thinking. All respondents thought that the simulation was challenging and that they enjoyed learning with it.

One more important finding in this study is related to the question about the most relevant attributes that would affect the chances of defense agents avoiding attacks until the end of the run. In the pre-simulation survey, the respondents expected that the most relevant parameter would be the defense Resources, followed by defense Skills and then Motivation. However, after trying the simulator, the respondents answered that defense Motivation was the most relevant parameter, followed by defense Skills and then the attack Motivation parameter. This shift from defense Resources to Motivation, and especially attack Motivation, shows that, at least from the preliminary results, the simulator was able to influence positively the respondents' way of thinking.

In the second experiment, we used the same tool and the target sample was composed of the members of the Norwegian team participating in the European Cybersecurity Challenge (ECSC 2018). The aim of this experiment was to measure the usability and extent of use of the tool for cybersecurity professionals and to understand team building in cybersecurity challenges. In this experiment, all ten participants used the simulator, separated into two groups, and nine of them subsequently responded to a survey.

The results from the second experiment showed that four respondents stated that the tool had developed their understanding of strategic management of information security but none of them agreed that the tool had increased their risk management knowledge. Four respondents did agree that the tool had developed their understanding of real world cyber scenarios. Regarding the process of adversarial thinking, five respondents agreed that the tool had improved their level of understanding, while three of them agreed on the question about systems thinking. Most respondents agreed that the tool was challenging but the majority were neutral about enjoying the learning process from the tool. In terms of the tool helping them improve their understanding of team building in cybersecurity challenges, only three respondents agreed on that, leaving space for further improvement in this direction.

Regarding the attributes involved, Motivation is the first ranked relevant attribute affecting both attack and defense agents' performance. So the most relevant attributes for the success of attack agents would be attack Motivation, followed by defense Motivation and attack Skills. For the defense side, the overall ranking put defense Motivation first, then attack Motivation followed by defense Skills. Finally, the respondents rated the usability and coverage of the simulation as average.

Furthermore, current results from the simulation experiments of the CyberAIMs version, with the risk quantification approach, show that defense agents with a low exposure factor (i.e. defense agents that implemented proper countermeasures and invested more efficiently in cybersecurity) have a higher "survival" rate than the ones with a high exposure factor. Besides the exposure factor, increasing the value of assets of defense agents, has a negative effect on their "survival" rate at the end of simulation time. In addition, the attack severity in this version, is influenced by the relative values of attributes of opposing agents, defining a built-in multiplier that ranges from 0.5 to 1.5.

5 Discussion

A realistic understanding of the level of cybersecurity risks is important because it is well known that inaccurate situational awareness often leads to incorrect decisions that can have catastrophic consequences. This requires cybersecurity decision makers to gain more knowledge about adversarial thinking, system thinking, and risk quantification. Modeling and simulation of real-world cyber-attacks is a useful training tool for the purpose of fulfilling these requirements [15].

Characterizing the behavior of attack and defense agents using resources, skills, and motivation during cyber-attacks is a key part of a comprehensive security model designed to carry out

quantitative security evaluations [16]. We believe that understanding the effects of these attributes can significantly improve cybersecurity decision making in businesses. The effectiveness of cyber defense in a business depends, to a large degree, on the ability of the business to assess – systematically and quantitatively – the impact of cyber attacks on its mission [17].

Hence, CyberAIMs can assist the cybersecurity decision makers in developing their adversarial and systems thinking skills, in addition to conducting experiments that make use of economic indexes and combined attack/defense perspectives during strategic decision making. Current results from experiments, and simulation runs of the different versions of the tool, show that CyberAIMs has had an overall positive impact on the users' understanding of the concepts related to adversarial and systems thinking; while it is also true that these results are certainly prone to additional implications, especially related to the small sample size and other factors. Moreover, the respondents were able to provide useful comments on the tool itself, including its design and the underlying features and value distribution of the attributes; these having been partly incorporated in the other version of CyberAIMs shown above. They will certainly be part of the future research into this topic.

6 Conclusions and Future Work

In our research, we presented how an STS approach can be used to design and support an agent-based simulation tool, CyberAIMs, in order to introduce the emerging role of systems thinking in cybersecurity education. We defined three main attributes, namely: Resources, Skills, and Motivation, which affect the behavior and performance of each actor within the simulation. Quantitative risk analysis is another part of CyberAIMs that enables the users to learn how implementation of proper countermeasures and precise asset valuation can affect the defense against cyber attacks.

The simulation tool presented in this article provides a solid basis for future research work in several directions. In future stages, based on the STS approach, we intend to look more deeply into the Motivation attribute, by conducting a more detailed literature review on the theories explaining attack actors' motivation, such as the ones related to the MOMM's taxonomy [18], and other theories explaining defense actors' motivation, such as the protection motivation theory [19]. Other potential extensions to this tool include calculating return on strategic security investment and return on attacks considering how vulnerabilities can be used for attacking multiple assets in an organization.

We will also develop the STS approach to address other cybersecurity challenges such as human behavior, organizational policies, and national strategies as well as monetary loss. This analysis can be extended to finding the best option in tackling cybersecurity risks (i.e. deter, protect, detect, response and recover). We will use the same approach to analyze and interpret findings from current and future versions of the tool that we have designed, in order to discuss the benefits of using STS in this area.

References

[1] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, vol. 5, pp. 10 862–10 868, 2011.

[2] "Curriculum guidelines for post-secondary degree programs in cybersecurity," *Cybersecurity Curricula 2017, Joint Task Force on Cybersecurity Education*, vol. 0.95, p. 21, November, 2017. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[3] H. J. Lawrence, A. Kirlik, Y. M. Goh, and P. Buckle, "Modelling and simulation of complex sociotechnical systems: Envisioning and analysing work environments." *Ergonomics*, vol. 58, no. 4, pp. 600–614, 2015. [Online]. Available: https://doi.org/10.1080/00140139.2015.1008586

[4] N. Kshetri, "Simple economics of cybercrime and the vicious circle," in *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives*. Springer, pp. 35–55, 2010. [Online]. Available: https://doi.org/10.1007/978-3-642-11522-6_2

[5] S. Kowalski, "It insecurity: A multi-disciplinary inquiry," *Royal Institute Of Technology, Sweden*, p. 1081, 1996.

[6] M. Rogers, "A new hacker taxonomy," *Department of Psychology University of Manitoba*, 2000.

[7] V. Pastor, G. Diaz, and M. Castro, "State-of-the-art simulation systems for information security education, training and awareness," in *IEEE EDUCON 2010 Conference, Madrid, Spain 14-16 April*. IEEE, pp. 1907–1916, 2010. [Online]. Available: https://doi.org/10.1109/EDUCON.2010.5492435

[8] U. Wilensky, "Netlogo," 1999. [Online]. Available: https://ccl.northwestern.edu/netlogo/

[9] N. Ben-Asher and C. Gonzalez, "Cyberwar game: A paradigm for understanding newchallenges of cyberwar," in *Cyber Warfare - Building the Scientific Foundation*. Springer, vol. 56, pp. 207–220, 2015. [Online]. Available: https://doi.org/10.1007/978-3-319-14039-1_10

[10] "Flipping the economics of attacks," Research Report, Ponemon Institute©, 2016.

[11] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002. [Online]. Available: https://doi.org/10.1145/581271.581274

[12] D. Tan, "Quantitative risk analysis step-by-step," 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849

[13] "Global cybersecurity index 2017," *ITU*. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

[14] E. Zoto, S. Kowalski, C. Frantz, E. Lopez-Rojas, and B. Katt, "A pilot study in cyber security education using cyberaims: A simulation-based experiment," in *IFIP World Conference on Information Security Education*. Springer, 2018, pp. 40–54. [Online]. Available: https://doi.org/10.1007/978-3-319-99734-6_4

[15] V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti, C. Sample, and S. Sugrim, "Simulations in cybersecurity: A review of cognitive modelingof network attackers, defenders, and users," *Frontiers in Psychology*, vol. 9, 2018. [Online]. Available: https://doi.org/10.3389/fpsyg.2018.00691

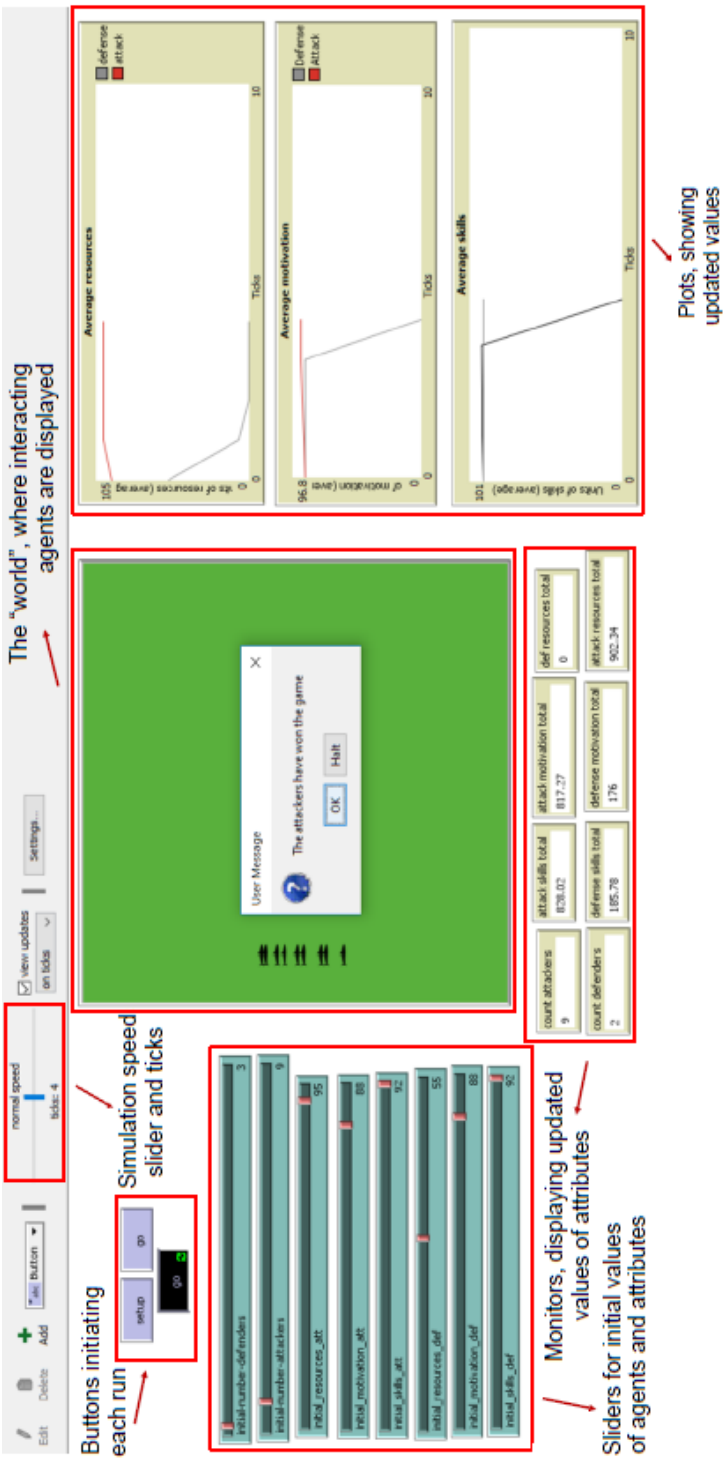
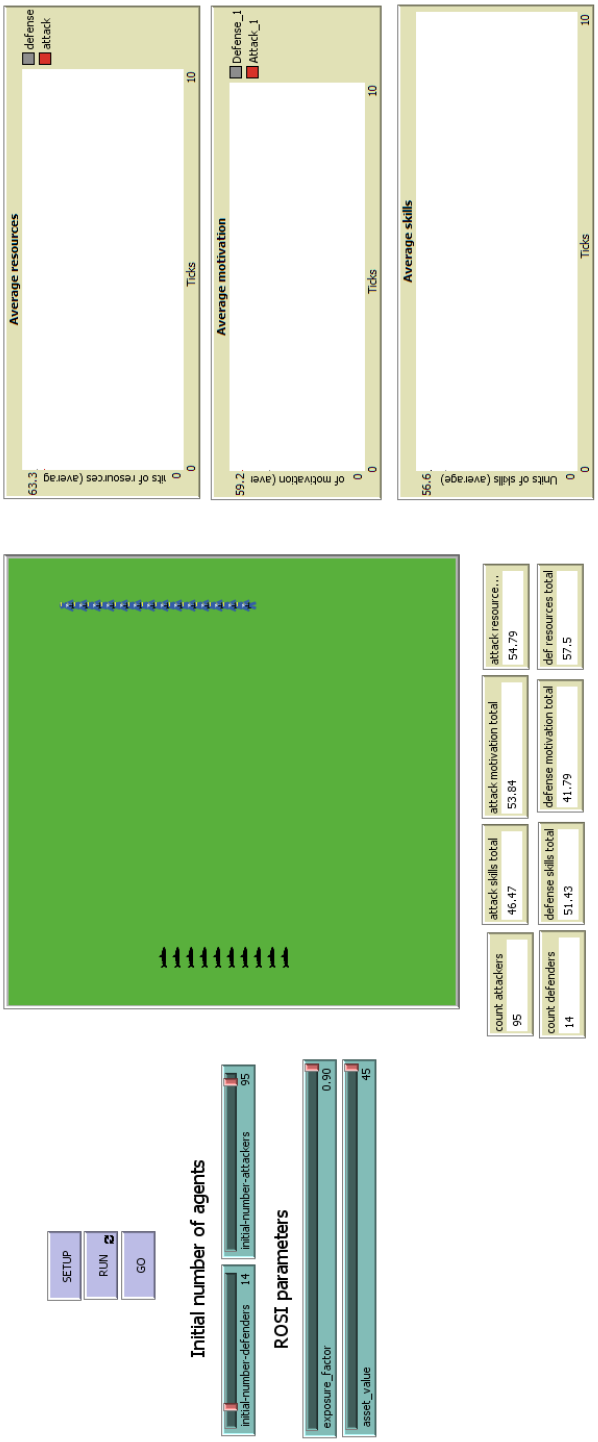
[16] E. V. Ruitenbeek, K. Keefe, W. H. Sanders, and C. Muehrcke, "Characterizing the behavior of cyber adversaries: The means, motive, and opportunity of cyberattacks," University of Illinois, 2010. [Online]. Available: https://www.perform.illinois.edu/Papers/USAN_papers/10VAN01.pdf

[17] A. Kott, M. Lange, and J. Ludwig, "Approaches to modeling the impact of cyberattacks on a mission," in *arXiv preprint arXiv:1710.04148*, Cornell University, 2017. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1710/1710.04148.pdf

[18] R. Zafarani, M. A. Abbasi, and H. Liu, "Momm's (motivations, opportunities, methods, means) – a taxonomy for computerrelated employee theft," *Journal of Assets Protection*, vol. 6, no. 3, pp. 33–36, 1981.

[19] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology. Interdisciplinary and Applied*, vol. 91, no. 1, pp. 93–114, 1975. [Online]. Available: https://doi.org/10.1080/00223980.1975.9915803

A Apendix: CyberAIMs Interface in NetLogo



B Apendix: Risk Quantification Interface in CyberAIMs