A Pilot Study in Cyber Security Education Using CyberAIMs: A Simulation-Based Experiment

Erjon Zoto, Stewart Kowalski, Christopher Frantz, Edgar Lopez-Rojas, Basel Katt

A Pilot Study in Cyber Security Education using CyberAIMs: A Simulation-Based Experiment

Erjon Zoto, Stewart Kowalski, Christopher Frantz, Edgar Lopez-Rojas, and Basel Katt

Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
[erjon.zoto;stewart.kowalski;christopher.frantz;
basel.katt;edgar.lopez]@ntnu.no

Abstract. We hardly pass any day without hearing of a new cyber attack. The recent ever-increasing occurrence of such attacks has given to researchers, practitioners and others an opportunity to raise awareness and train staff from the public and private institutions, as well as other people within the society, about the evolving nature of cyberspace threats. As a first step in this process, we aim to present main findings from a pilot study conducted with a target group of Master students with diverse backgrounds and knowledge about cyber security practices. The study was done using an agent-based simulation tool, CyberAIMs, as the core component of the experiment. Students were involved in a pre-test/post-test study in order to assess the probable change in their thinking process after using CyberAIMs. A scenario created from a real cyber case was additionally used to get the participants accustomed to the tool. The experiment is still in progress, while preliminary data indicate that there is a shift in students' perspective on the most relevant attributes affecting defense agents' performance, results that could be related to both adversarial and systems thinking processes.

Keywords: Agent-based simulation · Teaching · Cyber security · Adversarial thinking · Systems thinking · Training

1 Introduction

Cyber security events have been major headlines at an ever-increasing pace for the past recent years. Last year produced notable attacks such as WannaCry and NotPetya, while the most recent global event targeted from cyber attackers has been the Winter Olympic Games in South Korea this February.

With attacks intensifying in numbers and covering more and more unpredictable targets, researchers and practitioners are putting their best efforts in trying to raise awareness and train staff from the public and private institutions about the evolving nature of cyberspace threats. Several leading institutions from academia and beyond have already paved the way for further research related to cyber security [2] (p. 21).

In line with recent developments, the Joint Task Force on Cybersecurity Education (JTF), created in September 2015, has developed a new curriculum

volume, as part of its continuous efforts on the main purpose of developing comprehensive curriculum guidance in cyber security education [8]. The new curriculum volume introduces some new crosscutting concepts to deal with the evolving nature of cyberspace threats. These are:

- Adversarial thinking, as a process that considers the potential actions of the opposing force working against the desired result.
- Systems thinking, as a process that considers the interplay between social and technical constraints to enable assured operations.

The contribution of our work is directed towards the improvement of the adversarial and systems thinking ability in cyber security with focus on Master level students. This study was performed using an agent-based simulation tool, named CyberAIMs. The name is an acronym for Cyber Agents' Interactive Modeling and Simulation. It also shows that each actor in cyberspace follows certain procedures and strategies according to their own aims, as part of a higher entity or on individual basis. CyberAIMs was built using NetLogo[1], which is a programmable modeling environment for simulating natural and social phenomena. NetLogo is particularly well suited for modeling complex systems developing over time, with hundreds or thousands of agents, all operating independently.

We used this tool as the main component of of a simulation-based experiment conducted with students of Information Security, in order to further address their adversarial and systems thinking abilities. The target group included 12 individuals in an elective Master course that were asked to answer two surveys, pre and post-experiment, as well as a scenario of a recent real-world case of a cyber attack during the experiment. Students were intended to use CyberAIMs in order to give correct answers to the questions from the scenario.

1.1 Learning benefits

Pastor et al. [9] have done extensive research work on the available state-of-the art simulation tools that can be used on the purpose of teaching and training. They suggest that such simulation tools should be designed to have a extremely simple user-friendly interface and, at the same time, allow the user to obtain a deep understanding of the concepts.

Adversarial thinking has already been studied as an important skill for cyber security, Hamman et al. [7] propose that cyber security students should learn about basic game theory concepts in order to improve their strategic reasoning abilities. Similar to Schneider [12], our work aims to teach cyber security to students at university level.

Systems thinking has been associated to different areas of research since several decades now, and can also be relevant for information and cyber security. There are many examples where using simulations for teaching systems thinking, such as the work from Goodwin and Franklin [6], or the contribution from Anne Badoel and Haslett [3]. Their seminal work motivated our work further in this

[1] http://ccl.northwestern.edu/netlogo/

paper, while aiming to use simulation as part of the curriculum developed in the field of cyber security.

We aim to reflect the mechanisms behind the thinking processes above by using them within CyberAIMs, part of our recent research work done in the intersection between cyber security and related research fields.

1.2 Outline of the paper

We have organized the paper contents as follows. Section 2 will provide information on the main research question and methodology used. Section 3 will provide more details on the design process of the tool used and its main features. The final sections will conclude this paper by providing main insights from the pilot study and relevant discussions to help the reader get familiar with the next objectives of this research process as a whole.

2 Research methodology

2.1 Research questions

The main aim of this paper is to produce a proof of concept artifact that is able to show how a simulation tool can affect thinking processes of a group of students in cyber security. With this artifact we hope to address the new directions suggested in developing curriculum for cyber security in education. We have devised the following research question in order to achieve the objectives mentioned above:

- Research Question (RQ): How can we improve adversarial and systems thinking ability on students in cyber security?

This research question helps us understand the approaches that might help improve the learning process of adversarial and/or systems thinking for training and teaching purposes, as mentioned above. We have proposed a simulation tool, inspired from the work of Pastor et al. [9], that may prove to be useful in such case. We justify the use of the simulation tool further in section 4 by using the results from the pre-test/post-test study with the sample target. The process is explained in the next subsection below.

2.2 Research methodology

Besides using a simulation tool as an intuitive way to improve learning outcomes of a cyber security course, we saw the need to validate potential outcomes by conducting surveys before and after the tool was used from the target sample. The surveys included a set of similar questions and a set of different questions, according to the objectives of this study. Each student was asked to provide their ID as a means to uniquely identify them. The students were also asked if they wanted to receive via email a soft copy of their individual answers.

In the pre-simulation survey, there were three sections of open and closed questions, listed below:

– Learning from simulations
– About you
– Expectations from the model

In the first section, students were provided with two sets of statements and further asked to answer them using a 5-levelled Likert scale, with values ranging from strongly disagree to strongly agree. Table 1 gives details on all questions requiring Likert scale feedback from respondents.

Table 1. Pre-simulation survey questions using Likert scale

Section	**Question**	**Statements/Options**
Learning from simulations	I expect that the simulation will develop my	Problem solving skills; Planning skills; Understanding of cybercrime; Understanding of economics theories on cybercrime; Understanding of strategic mgmt. of info. security; Understanding of risk management; Understanding of real-world cyber scenarios; Understanding of systems thinking; Understanding of adversarial thinking
	Please rate your agreement with the following	The simulation will be challenging; I will enjoy learning with the simulation; Building on knowledge gained from previous courses; Building on knowledge gained from previous labs
About you	Please rate your agreement with the following	I have a background in programming; I have a background in economics/management; I have a background in human sciences/psychology; I have a background in military/warfare strategies
Expectations from the model	Please rate the level of relevance for each attribute on the attack success rate	Defense Resources; Defense Skills; Defense Motivation; Attack Resources; Attack Skills; Attack Motivation
	Please rate the level of relevance for each attribute on the defense success rate	Defense Resources; Defense Skills; Defense Motivation; Attack Resources; Attack Skills; Attack Motivation

The next section of this survey required feedback on the respondents current program of studies, home country, gender and age. It also included a question on the respondents' background using a Likert scale with same values as above.

The final section included two questions on the students' expectations related to the most relevant attributes. They had to provide answers using another 5-levelled Likert scale by rating all attributes given from highly irrelevant to highly relevant regarding their impact on each side's success rate, linked to the

probability of the simulation ending in fewer steps than the maximum available ones. Students were further asked to rank top three attributes that they thought were most relevant. They had also the opportunity to submit optional comments on the rationale behind the answers provided in this section.

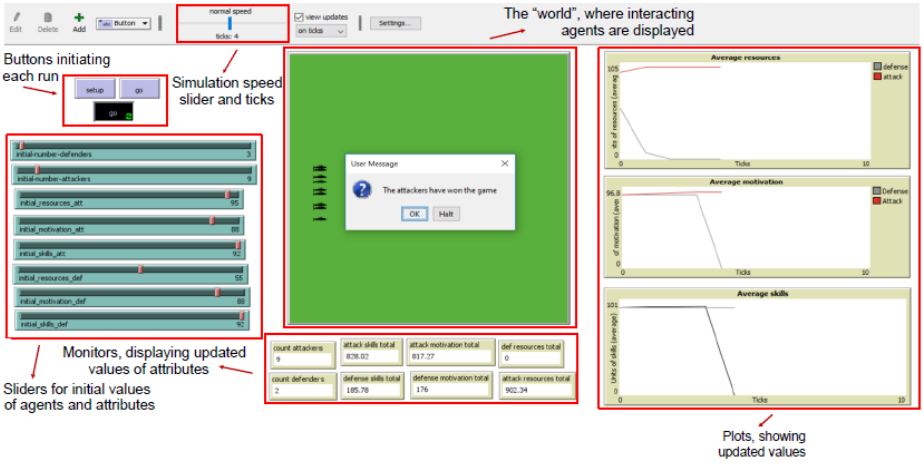
In order to simplify and improve the learning outcomes, we created a scenario related to a recent real-world case of a cyber attack, that could be easily mapped into CyberAIMs and further analyzed. The scenario was the main part of the lab conducted with the students, where they were asked to answer questions by putting into practice their knowledge on the tool and the logic behind the attributes involved. Questions included calculating the defense success rate and defining the most relevant attributes related to this rate. In the next section, we will provide more details about CyberAIMs.

The post-simulation survey included two sections of open and closed questions, similar to the first and last section of the pre-survey. The perspective changed from the expected to the real learning outcomes from using the tool. Here, in the final section, an additional question required respondents' feedback on the total time of engagement with the tool as well as a concluding optional comment on the whole experience related to the experiment.

3 CyberAIMs

CyberAIMs is an agent-based simulation tool designed in NetLogo, as shown in Figure 1. It includes two sets of agents, namely defense and attack agents. We classified each of the groups in four distinct categories, hereinafter echelons.

Fig. 1. Screenshot - CyberAIMs



Defense echelons are: *Ind* (individuals, ordinary people, related to a specific socio-cultural context), *SMB* (small and medium businesses, with relatively

low yearly income), *Corp* (multinational corporations, biggest enterprises), *State* (state agents, part of high-level organizations and agencies).

Attack echelons are: *Kid* (the script kiddies, individual hackers, also part of a specific socio-cultural context), *Ideol* (ideological hackers, hack-tivists, acting on the basis on moral and ethical duty), *Contract* (the Contractors, organized cybercrime groups, providing illegitimate services in exchange for money or other incentives), *State* (state-sponsored attack agents, high-level organizations and agencies, heavily engaged in cyberwar events recently).

We defined further three attributes to explain the behaviour and performance of the agents within CyberAIMs. The attributes are *Resources*, the budget related to cyber activities; *Skills*, the level of training, literacy and awareness on cyber events; and *Motivation*, the level of self-motivation and incentives in a certain time.

We used various sources of data for *Resources* depending on the agents' side and echelons, including the Ponemon Report [10], and also the GCI Index [5] for the *Skills* units. As an example, an individual spending 1000 USD would have 25 units of *Resources*, while a state spending USD 1 billion would have 75 units. Meanwhile, agents from Singapore, the country with the highest GCI score, would have on average 92 units of *Skills*. Finally, we used a heuristic approach for *Motivation* in this version of CyberAIMs, which only included a four-levelled scale from Low to High. In the next versions of the tool, we intend to use various motivation theories, as explained in the last section.

The current version of CyberAIMs allows the user to define initial number of agents in each side of the battlefield and also the initial value for each of the attributes for all agents on each side. The user can choose values in a [1 100] range for the number of agents on each side, initial units of *Resources* and *Motivation*, and a [1, 93] range for the *Skills* units, as detailed in Table 2.

Table 2. Distribution of attributes' values

Attribute	**Side**	**Echelon/ Level**	**Range of values**
Resources	Defense	Ind	1-31
		SMB	1-40
		Corp	40-70
		State	60-100
	Attack	Kid	1-37
		Ideol	15-37
		Contract	35-67
		State	60-100
Skills	Attack/ Defense	Low	1-30
		Medium	31-70
		High	71-93
Motivation	Attack/ Defense	Low	1-25
		Moderate Low	26-50
		Medium	51-75
		High	76-100

The tool performs each run in a period of max 120 ticks. Each tick represents a fixed period of time of three days, mapping the minimum time required for an attacker to perform a successful attack [10], thus making it able to predict the behavior of agents on both sides within a year. The current version allows a random attack agent on each tick to randomly target one or more defense agents, while attacking them depends on the combined attributes' values on each side.

If the attack is performed, the defense agent on target loses to the attacking agent a certain amount of *Resources*, related to to the attack agent's relative power, defined by multiplying the latter attribute values and dividing them by the sum of attribute values' products from both agents. The *Skills* units are also updated by increasing values in both sides, with the defense agent having a larger increase in terms of learning experience. *Motivation* units are also updated on the attack agents side, increasing them by the value of its relative power. If the attack is avoided, *Motivation* units are updated only on the defense side, by the value of the attack agent's relative power.

Continuous successful attacks can actually decrease defense agents' *Resources* units until losing them all. When this happens, the defense agent goes offline, meaning he does not interact anymore with the other agents. When all defense agents go offline, CyberAIMs stops running, displaying a message on the attack agents winning the game, as in Figure 1 above.

By having initial values of attributes comparable between them along with successful attacks defined by the simple product of attributes values, CyberAIMs aims to analyze the impact of initially equal attributes in the final outcome after each run. Furthermore, changing *Skills* and *Motivation* values along with *Resources* values helps create a more holistic approach to the problem in question. This is how we aimed to reflect the systems thinking concept within the tool, while *Resources* are more relevant only when comparing outcomes between attack agents of different echelons, with values of *Skills* and *Motivation* kept constant.

In terms of adversarial thinking, CyberAIMs allows the attack agents to decide if they want to attack their target opponents based on their attribute values. Thus, attack agents have full information on their opponents before taking the next step and they are able to think like their potential targets.

4 Study results

The target sample was composed from 12 students, attending the same course, while studying in several Masters' programs. Students had two hours of introduction to the tool developed, including the emerging concepts in cyber security curriculum related to systems and adversarial thinking. They were then asked to answer a pre-survey, followed by a scenario of a recent real-world case of a cyber attack during the experiment, and then the post-experiment survey.

4.1 Pre-simulation survey

We received seven surveys completed out of 12 (58,3% response rate) that will be part of the analysis below. The gender composition was two female and five male respondents. The age range of the respondents included values from 23 to 54 years old and the respondents were part of four different Masters' programs. Three students were non native, one of them being an exchange student.

Five students had a programming background, while one of them had it combined with a background in management or economics and another one had also a background in psychology or human sciences. Only one respondent had a strong military background and that was combined with a strong background in management or economics as well.

Regarding questions from the first section, six students expected the tool could help them develop their understanding of adversarial thinking and four of them agreed on the statement about systems thinking. On the other hand, only one student expected the simulation would develop his understanding on risk management.

Six students thought that the simulation would be challenging, while five of them thought they would enjoy learning with the simulation. Five students expected the simulation would build on knowledge from previous courses, while only three of them expected it would build on previous labs they attended.

In the last section, respondents answered that the defense *Motivation* was the least relevant attribute for the attack success rate, while attack *Resources* was the least relevant attribute for the defense success rate. The results show that the most relevant attributes affecting the attack success rate were *Motivation* and *Skills* of attack side and then *Resources* for the defense side. On the other side, the most relevant attributes expected to affect defense success rate were defense *Resources*, *Skills* and then *Motivation*.

Results from the first and last section were compared with results coming from the scenarios and post-simulation survey where appropriate.

4.2 Scenario results

The scenario was the main output of the lab conducted with the students, and we received answers from eight respondents out of 12 (66% response rate).

We prepared the scenario based on a real cyber case occurred recently, where an Iranian state-sponsored group was successful in targeting critical infrastructure entities in the US, Saudi Arabia and South Korea[2].

Thus, building on this real case, we asked the students to analyze these results using the simulation tool and values mapped from the actors participating there.

First, we instructed students on using the values shown in Table 3 to define initial units of *Resources* and *Skills* for each country or entity that was part of the scenario.

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

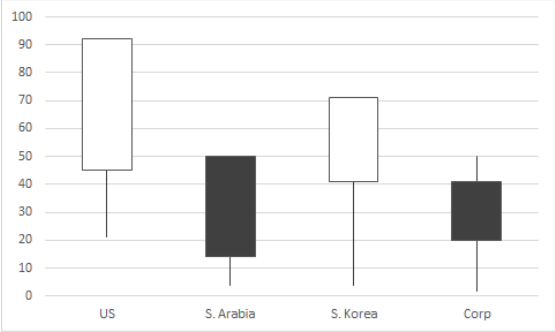
Table 3. Relevant values for the scenario

Entity/Country	Resources	Skills
US	98	91
Saudi Arabia	90	57
South Korea	88	78
Iran	84	49
Corporations	40-70	1-100

The values for the *Resources* are mostly related to the State agents values for each country, considering the companies were part of the critical infrastructure. Table 3 also includes values related to agents representing multinational corporations, since they could reflect same behavior with the ones targeted in the real attack. We suggested the *Skills* values above in order to think how the tool could help analyze the event explained in the scenario by using respective values from the GCI index, but we instructed the students on the best approach being to use distributed values of *Skills* and *Motivation* on both sides, so as to reflect the random distribution of values among different agents.

In the first question, we asked the students about the success rate of the defense agents involved in this scenario, whether they represented US, Saudi, Korean or corporations entities. The answers are summarized in the chart below.

Fig. 2. Defense Success rate (%) - Responses



The second question asked the respondents to submit initial attribute values on both sides for at least three cases when the attack agents succeeded in their attempts to win the battle, followed by at least three cases when the defense agents succeeded in their attempt to avoid being attacked. This question was considered relevant so as to make respondents think about potential patterns drawn from the values shown here and possible correlations between attributes and the final outcome in terms of each side's success as above. It was also useful in understanding how well the respondents followed the instructions given in the first question.

Following the same logic, the third question asked respondents to rank up to three of the six defined attributes (three on each side) as the most relevant ones affecting the chances of a defense agent to survive the whole run of 120 ticks, thus

his overall success rate. The results were quite different from the same question posed in the pre-simulation survey. They showed defense *Motivation* as the most relevant attribute, followed by defense *Skills* and then attack *Motivation*. Defense *Resources* was ranked fourth overall, thus a quite different outcome from the pre-survey, while a larger sample size would provide more meaningful results on this case.

4.3 Post-simulation survey

We have received only four surveys completed out of 12 (33% response rate) for the post-simulation phase, while a more detailed analysis will be part of the future stages of our research.

In the first section, two respondents stated that CyberAIMs developed their understanding of economic theories in cybercrime, while the others agreed on the simulation developing their own understanding of cybercrime. Three respondents agreed on the simulation developing their understanding on strategic management of information security, and two of them 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 out of four respondents agreed that the simulation did develop their understanding on 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. Only one respondent agreed on the simulation building on knowledge from previous courses and another one agreed on the statement regarding previous labs, with the other respondents not agreeing or being neutral.

In the last section, when asked about the level of relevance of all attributes in the attack success rate, the respondents agreed that the most relevant one is attack *Motivation*. The other attributes in the top three were attack *Skills* and defense *Motivation*.

On the other hand, when asked about the most relevant attributes on the defense success rate, all respondents seemed to agree on the most relevant attribute being attack *Motivation*, followed by defense *Motivation* and then defense *Skills*.

The current results from this section, even in this preliminary stage, could define a change in perspective between the pre-study and the post-study, supported from the lab conducted using the tool.

Meanwhile, the results from the question on the respondents' engagement with the tool show that respondents spent a total time between four to five hours on learning CyberAIMs and creating useful outputs from it. Thus, somewhat between one and two regular lecture sessions were seemingly enough to change their perspective as related to systems and adversarial thinking, though a larger sample size is needed to produce statistically more significant results on this direction.

5 Discussion and conclusions

Only three cases were valid for the whole process from the first to the second survey out of a total of 12 students in the course (25% rate). The answers on the most relevant attributes affecting defense success rate were the only connecting dots, while Table 4 shows the different responses before and after using CyberAIMs.

Table 4. Most relevant attributes on the defense success rate

Pre-survey responses	**Post-survey responses**
Defense *Resources*	Attack *Motivation*
Defense *Skills*	Defense *Motivation*
Defense *Motivation*	Defense *Skills*

Overall results reflect a better understanding of systems thinking, in terms of considering as most relevant attributes *Motivation* and *Skills* instead of *Resources* of each side, along with a better understanding of adversarial thinking, while thinking of attack attributes as equal or more relevant than defense ones on the defense side performance.

5.1 Additional comments

The results above are prone to additional implications. Only four students were able to compute decreasing success rates of the defense side between the scenarios in the first question. According to their comments on the results, it seems that two of them were not able to follow our instructions on how to perform the analysis, while the two others could not apply them in the correct way.

The respondents further enforced these issues in their comments on the final survey, establishing a potential direction for further improvements in the whole process.

There were also useful comments received on the tool itself, including its design and the underlying features and values' distribution of the attributes, which is already incorporated in the forthcoming version of CyberAIMs, part of the future research.

5.2 Conclusions

This paper aims to contribute on recent research done in respect to the learning benefits of simulation tools in cyber security education. The main outcomes of our pilot study point to a shift of the respondents' perspective after using the tool, indicating that CyberAIMs can have an effect on the students' understanding of systems and adversarial thinking. The results are however preliminary, while this tool will be further improved and designed to be used for larger sample sizes of students in related programs of study and potential cyber competitions.

We are already designing another version of CyberAIMs, using another approach towards a more realistic picture of the current cyberspace, based on the work of Ablon et al. in [1]. Furthermore, we intend to look deeper into the *Motivation* attribute, through a more detailed literature review on the underlying theories, such as the MOMMs taxonomy [4] and the protection theory [11].

We intend to use the feedback received from the overall process in order to increase response rates and increase the usability and coverage levels of the forthcoming versions of CyberAIMs.

References

1. Ablon, L., Libicki, M.C., Golay, A.A.: Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation (2014)
2. ACM: Computer Science Curricula 2013 Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. New York, NY, USA (2013)
3. Anne Bardoel, E., Haslett, T.: Success to the successful: The use of systems thinking tools in teaching ob. Organization Management Journal **1**(2), 112–124 (2004)
4. Bologna, J.: Momm's (motivations, opportunities, methods, means)-a taxonomy for computer related employee theft. Assets Protection **6**(3), 33–36 (1981)
5. Brahima, S.: Global cybersecurity index 2017. International Telecommunication Union (ITU) pp. 1–77 (2017)
6. Goodwin, J.S., Franklin, S.G.: The beer distribution game: using simulation to teach systems thinking. Journal of Management Development **13**(8), 7–15 (1994)
7. Hamman, S.T., Hopkinson, K.M., Markham, R.L., Chaplik, A.M., Metzler, G.E.: Teaching game theory to improve adversarial thinking in cybersecurity students. IEEE Transactions on Education **60**(3), 205–211 (2017)
8. Joint Task Force on Cybersecurity Education: Cybersecurity curricula 2017 - curriculum guidelines for post-secondary degree programs in cybersecurity - csec2017 v. 0.95 draft. Tech. rep. (Nov 2017)
9. Pastor, V., Díaz, G., Castro, M.: State-of-the-art simulation systems for information security education, training and awareness. In: Education Engineering (EDUCON), 2010 IEEE. pp. 1907–1916. IEEE (2010)
10. Ponemon Institute: Flipping the economics of attacks. Tech. rep. (Jan 2016)
11. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology **91**(1), 93–114 (1975)
12. Schneider, F.B.: Cybersecurity education in universities. IEEE Security & Privacy **11**(4), 3–4 (2013)

Appendix

A1. Pre-simulation Survey

Student ID number: _____
Note: this information will only be used to link your pre-simulation and post-simulation surveys and will not be retained for further analysis.

SECTION 1: LEARNING FROM SIMULATIONS
This section aims to get information on a 5-levelled Likert scale (strongly disagree - strongly agree) basis, according to your own perceptions and expectations. The Likert scale will be replaced by numbers, as follows:

strongly disagree	**disagree**	**neutral**	**agree**	**strongly agree**
-2	-1	0	1	2

1. I expect that the simulation will develop my:

	-2	-1	0	1	2
problem solving skills					
planning skills					
understanding of cybercrime					
understanding of economics theories on cybercrime					
understanding of strategic mgmt. of info. security					
understanding of risk management					
understanding of real-world cyber scenarios					
understanding of systems thinking					
understanding of adversarial thinking					

2. Please rate your agreement with the following statements:

	-2	-1	0	1	2
The simulation will be challenging					
I will enjoy learning with the simulation					
It will build on knowledge gained from previous groups					
It will build on knowledge gained from previous labs					

SECTION 2: ABOUT YOU
This section will require some personal information from you

1. Please tell us your gender:

- Female
- Male
- Prefer not to answer

2. In what year were you born? ____

3. If you are an international student, what is your home country? _____

4. What is the name of the degree you are completing? _____

5. Which of the following apply to you? (Select all that apply)

- I am studying part-time
- *I am studying externally (distance education)*
- *English is not my first language*
- *I am an International student*
- *I am working casually / part-time while studying*
- *I am working full-time while studying*
- *I am an exchange student*

6. Please rate your agreement with the following statements:

	-2	-1	0	1	2
I have a background in programming					
I have a background in economics or management sciences					
I have a background in human sciences/psychology					
I have a background in military/warfare strategies and rules					

SECTION 3: EXPECTATIONS FROM THE MODEL

This section requires information on your perceptions and expectations on a 5-levelled Likert scale (highly irrelevant - highly relevant) basis, related to the model features explained before the lab.The Likert scale will be replaced by numbers, as follows:

highly irrelevant	**irrelevant**	**neutral**	**relevant**	**highly relevant**
0	1	2	3	4

1. Please rate the level of relevance for each attribute on the attack/defense success rate:

Attack	0	1	2	3	4	Defense	0	1	2	3	4
Defense Resources						*Defense Resources*					
Defense Skills						*Defense Skills*					
Defense Motivation						*Defense Motivation*					
Attack Resources						*Attack Resources*					
Attack Skills						*Attack Skills*					
Attack Motivation						*Attack Motivation*					

2. What do you expect to be the top 3 attributes for the attack agents' success rate?

Example: a. attack resources; b. defense skills; c. defense resources;

a. _____
b. _____
c. _____

3. What is the rationale behind your selection above?

---

4. What do you expect to be the top 3 attributes for the defense agents' success rate?
Example: a. attack resources; b. defense skills; c. defense resources;

a. _____
b. _____
c. _____

5. What is the rationale behind your selection above?

Thank you for your participation!