CYBER RESILIENCE AWARENESS TRAINING CYBER RANGE

Juan F Carías[1], Marta Iturriza[1], Saioa Arrizabalaga[1,2] and Josune Hernantes[1]
University of Navarra, TECNUN, School of Engineering[1]
CEIT BRTA[2]
jfcarias@tecnun.es

Abstract
The massification of technology in almost every aspect of life has brought a worrying cyber scenario where thousands of resources are invested either to prevent cyber incidents or to pay for the damages that they cause. This situation affects cities since the main city stakeholders are the citizens and public and private organizations. Therefore, these stakeholders need to be aware of the risks they face and consider their responsibility in adopting measures to be safe in the dangerous cyber scenario. This responsibility is especially relevant for organizations (public and private) since they provide services that ensure the wellbeing of other stakeholders (other companies and citizens), especially critical infrastructures. In this sense, most organizations still consider a cybersecurity approach where the objective is to be "fail-safe". However, considering the rapid evolution of technology and cyber threats, this approach can be naïve since it is unlikely to protect against all the threats and vulnerabilities that every system has. Instead, the cyber resilience approach would be much more flexible since organizations would not seek to be "fail-safe", but "safe-to-fail". Nevertheless, cyber resilience operationalization is not easy since it involves multiple dimensions that are complex and form complex interrelationships. Thus, decision-makers need tools to understand the effects of their investments (or lack thereof) in cyber resilience operationalization. These tools would increase the awareness of these decision makers, which would in turn help them operationalize cyber resilience with more informed criteria. This article proposes the use of system dynamics models in virtual cyber ranges as the tools to increase the decision-makers' awareness. The usage of virtual cyber ranges lets decision-makers experiment with different approaches to the operationalization of cyber resilience without risking real organizations' assets. This approach could help them increase their awareness and develop effective strategies to become more cyber resilient.

Keywords: Cyber Resilience, Cyber Range, Awareness, City Resilience, System Dynamics

Introduction
Cyber incidents have been among the most relevant global risks for the last couple of years because they are among the risks with highest impact and probability of occurring (World Economic Forum, 2020). Moreover, the traditional way of approaching security towards these threats was being fail-safe by protecting against them and covering all the vulnerabilities (Björk et al., 2015). However, due to the rapid evolution of technology, the increased exposure to it and the rapid adaptation of cybercriminals to the new vulnerabilities it is becoming increasingly difficult to be completely fail-safe. For this reason, a new approach is required in which technical protection of the systems is accompanied with systematic strategic and organizational planning to develop capabilities that make systems safe-to-fail. This approach is called cyber resilience (Björk et al., 2015). In this sense, a formal definition of the concept

[1] Paseo Manuel Lardizabal, 13. 20018. San Sebastian, Spain.
[2] Paseo Manuel Lardizabal, 13. 20018. San Sebastian, Spain.

is the "ability of a process, business, organization, or nation to anticipate, [detect], withstand, recover, and evolve in order to improve their capabilities in face of adverse conditions, stress, or attacks to the cyber resources it needs to function" (INCIBE, 2019). This definition reflects its holistic nature and its objective of making different kinds of systems (such as processes, businesses, etc.) safe-to-fail.

Cyber incidents affecting companies can be worrying for cities since these companies can be public, private or even critical infrastructures. These companies provide services to ensure the wellbeing of All city stakeholders since the main city stakeholders are citizens, public and private companies (Iturriza et al., 2020) cities are indeed vulnerable to cyber incidents because both companies and citizens can be compromised by cyber incidents. Among these stakeholders, companies are the most relevant because these are more likely to be attacked (Allianz, 2020) and they have to look after themselves and their employees, clients, etc. which are either citizens or other companies. Thus, this study focuses mainly on companies.

In this sense, companies require cyber resilience to protect themselves, other companies and citizens from cyber incidents whichever their cause. However, cyber resilience operationalization is complex because of its multi-dimensional and holistic concept (Dupont, 2019). Cyber resilience operationalization requires knowledge and awareness from the decision-makers since in this concept technical solutions are only part of the equation and both human contribution and strategic planning play an important role in the development of cyber resilience capabilities (Deutscher et al., 2017).

The difficulty of operationalizing cyber resilience has encouraged the current literature to lean towards frameworks, standards and other documents that enumerate the multiple dimensions and policies needed to develop cyber resilience (NIST, 2018). However, most of these aiding documents do not help companies prioritize these dimensions and policies and leave that decision to the company implementing them (MITRE, 2012; NIST, 2018). Although this is reasonable because of the varied circumstances the companies implementing these dimensions and policies could be in, it is also difficult to prioritize these policies when there is a lack of specialized personnel and resources dedicated towards cyber resilience such as in the case smaller companies (Ben-Asher and Gonzalez, 2015). In this sense, previous research has proposed System Dynamics (SD) as a plausible tool to let decision makers gain this knowledge and awareness needed to understand the consequences of their investments (or lack thereof) and thus prioritize and strategize their cyber resilience operationalization more effectively (Carias et al., 2019).

Thus, the purpose of this article is to use SD to develop a cyber resilience cyber range as a tool to increase the decision-makers' awareness and in this way build cyber resilience in companies and potentially cities. In this sense, the tool proposed in the article could help decision-makers better understand the interrelationships between the cyber resilience policies and the consequences of their decisions. This could later help them create effective strategies towards the cyber resilience operationalization in their environment.

State of the art

The current literature contains several documents with the objective of aiding companies in cyber resilience operationalization (frameworks, maturity models, self-assessment questionnaires, standards, metrics, etc.). Some examples are NIST's Cybersecurity Framework, Cybersecurity Capability Maturity Model (C2M2) and the Cyber Resilience Review (CRR) from the Software Engineering Institute at Carnegie Mellon University. Although useful, the existing documents often limit to enumerating the policies or actions that companies should implement to develop cyber resilience. However, most of them explicitly require customization through the selection of a set of policies, actions or metrics that apply to the current situation that the entity implementing them is in (MITRE, 2012; NIST, 2018). In order to correctly prioritize these policies, experience and knowledge are required, but most companies usually lack the specialized personnel to effectively prioritize these policies (Ben-Asher and Gonzalez, 2015). Therefore, training and awareness tools for decision-makers to better understand the complex cyber resilience concept are needed (Dupont, 2019; Jalali et al., 2019).

In this vein, cyber ranges are virtual environments in which a trainee can embark on hands-on activities and through them gain practical knowledge in cyber security (Pham et al., 2016). A broader concept related to cyber ranges is the concept of serious games. This concept is used in other areas and defined

as an "interactive system based on a set of agreed rules and constrains, directed toward a clear goal often set as challenge" (Malone, 1981). Other more modern definitions of this concept also include computer and video game characteristics (De Freitas and Jarvis, 2007). Since cyber ranges are a particular case of serious games, as their definitions suggest, this article uses both terms interchangeably.

Moreover, serious games enable users to better understand the problem at hand, to train themselves to take more appropriate decisions and to get to know the system under study (Arnab et al., 2015; Jalali et al., 2019). Consequently, the learning process and the assimilation of the concepts presented are facilitated (Arnab et al., 2015). In this vein, Ke (2009) pointed that the content and context of the serious game are key in order to accomplish the aim of the tool. Sitzman (2011) added the necessity of serious games to be designed as an active learning tool and the importance of having them combined with other tools that complement the education and training process. On top of that, Hamari (2014) stated that the most successful and used serious games were the ones simulating real world tasks and giving instant feedback of the process.

In this vein, a few examples of serious games can be found in the literature focused on the cyber resilience context. Lee Urban et al. (2016) presented two simulation approaches to analyze the effects of cyberattacks on a network. However, the aim of their study is to develop simulations to analyze a specific sector whereas the aim of this article is to design serious games to train and educate decision-makers in cyber resilience management and operationalization from an aggregated perspective.

Omerovic et al. (2019) developed a modelling approach to conduct risk analysis of cybersecurity in the context of smart power grids. Nevertheless, the study is still on going and no interface and final serious game have been presented yet.

Finally, Jalali et al. (2019) presented a serious game to study the effectiveness of the decisions taken by the experts concerning two cybersecurity capabilities: potential delays in capability development and uncertainty in cyber incidents prediction. Their research highlighted the importance of training to understand cyber complexities and the potential of serious games to do so.

Therefore, recent research highlights the potential of serious games application to facilitate decision-makers see the short, mid, and long-term effects of their decisions, understand the interrelationships between cyber resilience policies and dimensions, etc. without risking real organizations' assets (Łatuszyńska, 2017). Consequently, decision-makers using the serious game will have complementary information to develop effective strategies to operationalize cyber resilience in their organizations or at least become more aware of the importance of each dimension and policy in the operationalization of cyber resilience. In this vein, the use of this approach could potentially help all types of city stakeholders to increase their awareness and develop effective strategies to become more cyber resilient. Yet, there is still a lack of examples and studies need to be conducted in the field.

In light of this situation, this article presents the use of simulation models encapsulated in an interface to be used by decision makers as a cyber range to increase cyber resilience awareness and support strategies for operationalization.

Methodology

The development of the cyber range was done in two steps. First, the System Dynamics methodology was used to develop models that represented the consequences of common decisions that cyber resilience managers make. Second, the development of a graphical interface for these models. The detailed process for each of these steps is summarized in Figure *1* and explained in the following subsections.

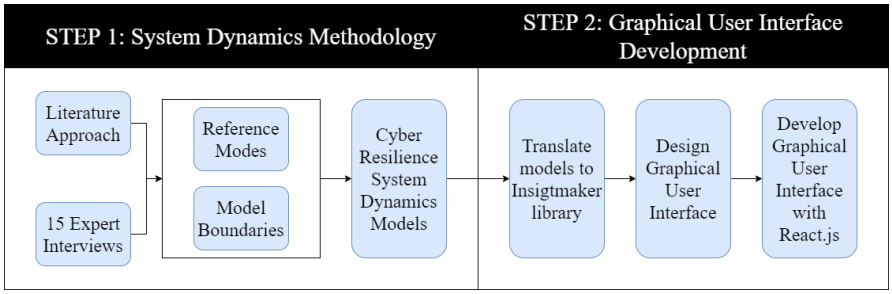

Figure 1 Summary of the employed methodology

STEP 1: System Dynamics Modelling

To develop models that would later be translated into a serious game to increase awareness of city stakeholders from public and private organizations this article used a System Dynamics (SD) methodology. In this sense, in addition to a literature review, 15 expert interviews were conducted to elicit their mental model and tacit knowledge concerning the investment decisions for improving cyber resilience. This is a known process in the SD model building, as many SD modelers admit that the knowledge of the stakeholders who have first-hand experience in the subject is required to structure and parameterize a useful model (Ford and Sterman, 1998).

SD modelling and simulation has frequently been used to illustrate the dynamics and the trade-offs between different competing decisions and options over time. SD simulation technique is also often considered as a safe environment to conduct experiments, test decisions, and observe the consequences on a system (Łatuszyńska, 2017). Moreover, one of the SD strengths is its ability to model socio-technical systems and dealing with the soft variables that are hard to quantify but are often influential to determine the behavior of variables under study (Forrester, 1980). Given the ability to show trade-offs and model mixed numerical and soft variables such as the ones found in cyber resilience operationalization the method is deemed to be appropriate for the purpose of this paper.

The combination of written databases (literature approach) and mental databases (expert interviews) was used to construct the cyber range. First, a literature approach was done to find interrelationships and known behaviors discussed in the literature. Previous research and the cyber resilience aiding documents discussed in the state of the art were used to find interrelationships between cyber resilience policies. Other articles, such as the ones mentioned in the state of the art, discussing interrelationships between policies and the importance of certain policies were also studied before comparing and contrasting with the experts' opinions on the important relationships and effects of cyber resilience policies.

Second, 15 expert interviews were conducted. These 15 experts were not only knowledgeable in the area of cybersecurity but also have experience in managing cyber resilience in business environments. In other words, they are familiar with the consequences of different decisions and options to businesses and companies.

The aims of the interviews with the experts for knowledge elicitation were twofold: First, to derive behavior over time (BoT) which is required in the SD method (Richardson and Pugh, 1981) to describe the dynamic of the problems being modeled. Second, to validate that the boundaries of the model and the time horizon that would be applied in the cyber resilience model were plausible. The elicitation process was designed to allow the experts drawing the Behavior over Time (BoT) as input for the model to represent the reality. Despite the chart not being an exact quantitative representation, it is vital to understanding the dynamics of managing cyber resilience (Forrester, 1980).

STEP 2: Graphical User Interface Development

In order to develop a graphical user interface (GUI) for the models to be used by city stakeholders from public and private companies, the models were translated into the Insightmaker library. This is a free, open source library that permits the development and later export of customized models that can be later executed through custom JavaScript code but maintaining the model's logic and behavior.

After exporting the model as required by the Insightmaker library, a user interface was designed in order to make the use of the model as intuitive as possible. To achieve this, sliders with percentages were used as the tool for decision-makers to select which policies they were going to invest in. Once the decision makers were satisfied with the balance of their investment, they had to be able to run the model. To do this, they only had to press a button with the clear "Simulate" statement and the model would be drawn on their screen according to the selected inputs. With this design in mind, the React.js front-end development framework was used to create the user interface.

Results: Cyber Range

As a result, of the previously described methodology, several interrelationships between cyber resilience policies were identified from the literature and from the expert interviews. The interrelationships between the policies led to the development of reference modes that could be modelled and therefore several models showing these reference modes and interrelationships were developed. These models were translated into the Insightmaker modelling and simulation engine and an interface was developed in order for decision-makers to be able to experiment with these. The models with interfaces can be used as serious games or cyber ranges to raise awareness amongst city stakeholders in the field of cyber resilience.

To instantiate these results, one model will be explained with the behaviors it encompasses and the lessons that a decision-maker could learn by using it in the following subsections.

CR Model

The model selected to exemplify the serious game involves five input variables, which represent investment in five possible cyber resilience policies. These five policies are: detection processes and continuous monitoring, information security, training and awareness, vulnerability management, and information sharing.

Based on the reference modes a Causal Loop Diagram (CLD) explaining the interrelationships between these five policies was developed and is shown in Figure 2.This CLD mainly shows how investments in cyber resilience policies can reduce the impact of cyber incidents in a company. In this particular case, impact also represents resources that are spent unnecessarily.

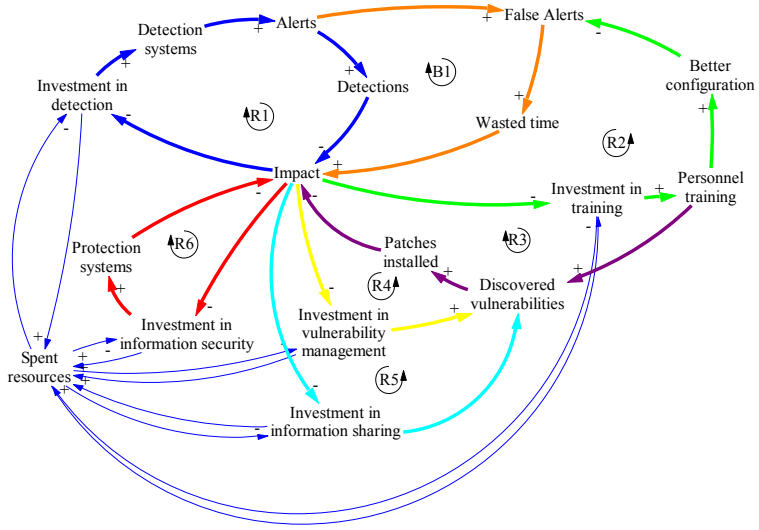

Figure 2 Causal Loop diagram

In the CLD, arrows represent causal relationships between variables, and the (+) or (-) signs represent whether the relationship is directly proportional (+) or inversely proportional (-). These causal relationships form causal loops that can either represent reinforcing behaviors (exponential or decaying behaviors) or balancing behaviors (limiting behaviors).

As marked in Figure 2, seven main behaviors (causal loops) represent the effects of the investments decision-makers can make and the interactions between these investments and the other policies. The marked causal loops are mostly reinforcing loops. These are not the only behaviors the model represents since there are several balancing loops that represent the limitation of resources. However, these balancing behaviors will not be explained in detail, as the aim of the article is to highlight the interrelationship between cyber resilience policies.

As mentioned before, the seven main behaviors that represent the effects of decision-makers' investments and their interactions are marked in Figure 2. As the figure shows, these are highlighted in different colors and have been numbered for reference. These causal loops can be explained as follows:

R1: Investment in detection processes and continuous monitoring allows the company to buy more detection systems. The more detection systems a company has the more alerts they generate. These alerts lead to detections and detecting incidents in time reduces their impact. Since there is less impact after investing in this domain, the decision-maker will likely invest in this domain again, thus the last causal relationship being inversely proportional (less impact, more investment in detection).

B1: This loop balances the investment in detection systems. Following the loop shows that half of it is shared with loop R1. This loop shows that the more investment in detection, the more detection systems. The more detection systems, more alerts will be issued by these systems. The more alerts there are, the more false alerts there will be. More false alerts will represent more wasted time spent checking these alerts and their cause. More wasted time will increase the impact because this time costs resources to the company. Opposite to the R1 loop, more impact will discourage the decision maker to invest in the same domain again.

R2: This loop represents how training can mitigate the effects of B1. R2, R1 and B1 together represent a behavior well known to the cybersecurity literature (Ben-Asher and Gonzalez, 2015). As shown in R2, investment in training will represent better trained personnel. Having better trained personnel can help better configure the detection systems, reducing the false alerts. Reducing the false alerts reduces the time wasted and this reduces the impact. Since investing in training reduces the impact, the less impact the more investment in training.

R3: This loop is another direct effect of training. In this case, it represents the relationship between training and vulnerability discovery. The more investment in training, the more trained the company's personnel will be. The more trained the personnel the better they will be to identify vulnerabilities. The more discovered vulnerabilities the more patched vulnerabilities there will be. As there are more patched vulnerabilities it is less likely to have a cyber incident and thus the less impact. The less impact there is the more investment in training because it worked.

R4: This loop represents the direct effect of investing in vulnerability management. In this case, investment in vulnerability management leads to more discovered vulnerabilities. More discovered vulnerabilities will mean that more systems are patched. Patched systems are less likely to be exploited, and therefore there will be less impact from cyber incidents. Less impact will lead the decision-maker to invest more in vulnerability management because it worked.

R5: This loop represents the effects of investing in information sharing. This loop is a simplification that assumes that the only direct effect of information sharing has to do with discovering vulnerabilities. Having said this, in the model R5 is also related to R4 because it assumes that the information received from third parties is exclusively about vulnerabilities. This means that the more investment on information sharing, the more discovered vulnerabilities. The more discovered vulnerabilities, the more patches installed. More installed patches reduce the likelihood of having cyber incidents, thus reducing the impact. Less impact will encourage the decision-maker to invest more in information sharing.

R6: This final loop represents the effects of investing in information security. In this sense, the more investment in information security the more protection systems the company will have. The more protection systems, the less likely it is to have a cyber incident and therefore the less impact there is. Less impact will encourage the decision maker to invest more in information security.

Graphical user interface

Using the described model as a base, an interface for de decisions makers has been developed as shown in Figure 3. When the decision-makers open the interface, the input variables of the model are shown in sliders with a scale of 0-100%. In these sliders, the decision makers can allocate their budget until they complete a 100% total and click simulate. If the decision-makers do not wish to allocate all the budget they can allocate as much as they want and click simulate.

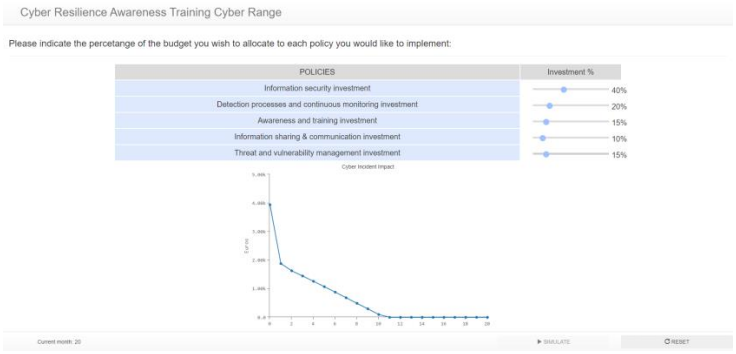

Figure 3 Serious Game Interface

In the case of the previously described model there are five input variables. Hence, there are five sliders on the decision-maker's screen to allocate budget to each one of them.

Furthermore, once the decision-makers click on the simulate button a graph of the impact over the course of 20 months is shown on screen. The impact of cyber incidents over time will depend on the allocation selected by the decision-makers and thus they will be able to re-adjust their decisions and experiment with different allocations and dynamic investment strategies to try to minimize the costs due to impact as soon as possible. In this process, the decision maker can learn the effects described in the model that are the theoretical interrelationships between cyber resilience policies. For instance, if the decision-maker allocates 100% of the budget to detection during the complete simulation, they would find out that the impact increases with respect to the original situation after a slight decrease, because without the adequate training, the false alerts consume resources and time that cost money to the company. This effect is shown in Figure 4. Although in this case only one variable is shown other variables could be graphed to further stress this effect.

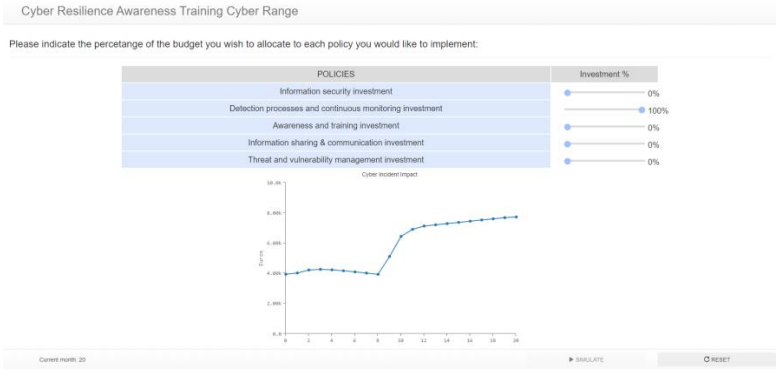

Figure 4 Allocating 100% of the budget to detection

As in this example, the other theoretical behaviors of cyber resilience policies can be shown by the serious game representing better or worse prioritization of the required policies.

Discussion

The literature suggests that the keys for a serious game to be useful are their content and context (Ke, 2009), their combination with other aiding tools that complement the training process (Sitzmann, 2011), and their representation of real world tasks with instant feedback (Hamari et al., 2014). Thus the discussion of this article will be outlined by these three characteristics.

First, the example serious game presented in this article represents the theory gathered from the literature and experts' experience. These behaviors are directly related to the ideas behind the cyber resilience frameworks and aiding documents that can be found in the literature. In fact, the interrelationships between cyber resilience policies represented in the models are a byproduct of the development of both an implementation order and a progression model for cyber resilience policies (Carias et al., 2020). Thus, the content and context are based on real experience from practitioners and contrasted with the current literature on the field. This makes the context and content of the cyber range rich and realistic fulfilling the key highlighted in Ke (2009).

Furthermore, this result is not isolated from other kinds of aiding documents for cyber resilience operationalization. Instead, these kind of models and interfaces can be used to complement them by letting decision-makers understand the "why" behind the "what" to do and the guidelines for prioritization and strategic planning given by other resources in the literature. This would make their cyber resilience operationalization better since it could avoid naïvely using these tools and guidelines without adapting to the circumstances. Thus, the results presented in this article are complementary to other aiding tools for decision-makers to enrich their learning process. This fulfills the key presented by Sitzmann (2011).

Finally, the cyber range in this article represents realistic behaviors of a system with which decision-makers might have previous experience. For instance, the limitation of resources is represented explicitly through loops between investments and spent resources. However, it is also worth noticing that there are more balancing loops showing that investing more in any given policy requires to invest less in other policies. This can be understood as a "tragedy of the commons" system dynamics archetype (Braun, 2002) and it is a simple representation of a balancing behavior that most people are familiar with and that is important to acknowledge when making decisions about investments in any area. Thus, the realistic characteristics brought by the experts and these familiar behaviors combined with the instant feedback from the model fulfill the third key as presented by Hamari et al. (2014).

Therefore, these serious games can be useful in the training and awareness building process of decision-makers for cyber resilience operationalization. On the one hand, they directly help them understand the effects of their investment (or lack thereof) in cyber resilience policies. On the other hand, these models can help them understand the reasons for the progressions of certain policies and the importance of their implementation order. For instance, using the example serious game as a reference, a decision maker can easily become aware that investing in training without investing before on detection systems or vulnerability management is not ideal.

Although this article uses one example to represent the benefits of using these serious games, the variety of behaviors that can be represented by different models and interfaces could be used to help decision-makers understand more about cyber resilience. This means that although this article is mainly focused on companies, cyber ranges for all types of city stakeholders could be made to increase their understanding and awareness of cyber resilience operationalization.

Having discussed the multiple advantages that using the results presented in this article could have, it is important to highlight that there are limitations to these models and interfaces. One of the limitations is that the results presented in this article have not been tested with a real company's data to calibrate the models to be as accurate as possible. This would be a good reality check for the models and would add value to the lessons that decision-makers could acquire from the serious games. On the other hand, although these models have been proven to help in other areas as discussed in the state of the art, it is still necessary to reaffirm this conclusion with studies done in the area of cyber resilience.

Conclusion

This article proposes a cyber resilience SD model with an interface as a cyber range to increase the awareness of city stakeholders (especially decision-makers from public and private companies). This cyber range proves to be versatile enough to encompass the complex interrelationships between the cyber resilience policies. Thus, the use of this serious games can be especially helpful to understand the consequences of investments (or lack thereof) and behaviors of a system when certain investments are made in these policies.

These results can not only improve the knowledge and awareness of decision-makers but also reinforce the implementation of other cyber resilience operationalization aiding tools in the current literature. In fact, these tools complement each other because these models are based on causal relationships that might show decision-makers the "why" they are encouraged by other guidelines to operationalize cyber resilience by implementing certain cyber resilience policies, implementing them in a certain way and in a certain order.

In this article, the shown cyber range represents the interrelationships and behaviors generated by the investments of a decision maker in five cyber resilience policies. This specific cyber range can increase the decision-makers' awareness over the importance of a dynamic and diversified investment to achieve better results, but also teaches about the importance of certain investments before others and how the limitation of resources affects the system. All these behaviors are realistic since they are either consequences of limited resources (a well-known phenomenon) or based on literature and 15 experts' inputs. Therefore, by using this specific model, decision-makers could understand why they should implement these policies and create effective strategies to do so. Like in this example, several other cyber ranges with different important lessons for city stakeholders could be used to develop the needed awareness for an effective cyber resilience operationalization.

In order to explore the reach of these results and reaffirm their validity, further research should aim towards two main branches. The first branch should validate the models by calibrating them with real information and make reality checks to make sure that the lessons that decision-makers extract from the serious games are directly applicable in a real situation. The second should confirm that serious games in the area of cyber resilience are as effective in building awareness for decision-makers as they have proven to do so in other areas.

References

Allianz. (2020). *Allianz Risk Barometer - Identifying the major business risks for 2020*. *25*, 1–11. http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometerTopBusinessRisks2016.pdf

Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., De Freitas, S., Louchart, S., Suttie, N., Berta, R., and De Gloria, A. (2015). Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology*, *46*(2), 391–411. https://doi.org/10.1111/bjet.12113

Ben-Asher, N., and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Björk, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, *353*(January), III–IV. https://doi.org/10.1007/978-3-319-16486-1

Braun, W. (2002). The system archetypes. *System*, *2002*, 27. http://www.albany.edu/faculty/gpr/PAD724/724WebArticles/sys_archetypes.pdf

Carias, J. F., Arrizabalaga, S., Labaka, L., and Hernantes, J. (2020). Cyber Resilience Progression Model. *Applied Sciences*, *10*(21), 7393. https://doi.org/10.3390/app10217393

Carias, J. F., Labaka, L., Sarriegi, J. M., and Hernantes, J. (2019). Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors*, *19*(1), 138. https://doi.org/10.3390/s19010138

De Freitas, S., and Jarvis, S. (2007). Serious games - Engaging training solutions: A research and development project for supporting training needs: Colloquium. *British Journal of Educational Technology*, *38*(3), 523–525. https://doi.org/10.1111/j.1467-8535.2007.00716.x

Deutscher, S. A., Bohmayr, W., and Asen, A. (2017). Building a Cyberresilient Organization. In *BCG Perspectives*. https://image-src.bcg.com/Images/BCG-Building-a-Cyberresilient-Organization-Jan-2017_tcm26-186244.pdf

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), 1–17. https://doi.org/10.1093/cybsec/tyz013

Ford, D. N., and Sterman, J. D. (1998). Expert knowledge elicitation to improve formal and mental models. *System Dynamics Review*, *14*(4), 309–340. https://doi.org/10.1002/(SICI)1099-1727(199824)14:4<309::AID-SDR154>3.0.CO;2-5

Forrester, J. W. (1980). Information Sources for Modeling the National Economy. *Journal of the American Statistical Association*, *75*(371), 555–566. http://www.jstor.org/stable/2287644

Hamari, J., Koivisto, J., and Sarsa, H. (2014). Does gamification work? - A literature review of empirical studies on gamification. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3025–3034. https://doi.org/10.1109/HICSS.2014.377

INCIBE. (2019). *Indicadores para Mejora de la Ciberresiliencia (IMC)*. https://www.incibe-cert.es/guias-y-estudios/guias/imc-indicadores-mejora-ciberresiliencia

Iturriza, M., Labaka, L., Hernantes, J., Abdeltawad, A., and Abdelgawad, A. (2020). Shifting to climate change aware cities to facilitate the city resilience implementation. *Cities*, *101*(February), 102688. https://doi.org/10.1016/j.cities.2020.102688

Jalali, M. S., Siegel, M., and Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Ke, F. (2009). A qualitative meta-analysis of computer games as learning tools. In *Handbook of research on effective electronic gaming in education (3 Volumes)* (Issue January 2009). https://doi.org/10.4018/978-1-59904-808-6

Łatuszyńska, M. (2017). System Dynamics Modeling in Behavioral Decision Making. In K. Nermend and M. Łatuszyńska (Eds.), *Neuroeconomic and Behavioral Aspects of Decision Making* (pp. 243–253). Springer International Publishing.

Lee-Urban, S., Whitaker, E., Riley, M., and Trewhitt, E. (2016). Two Complementary Network Modeling and Simulation Approaches to Aid in Understanding Advanced Cyber Threats. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 401–414). Springer International Publishing.

Malone, T. W. (1981). Toward a theory of intrinsically motivating instruction. *Cognitive Science*, *5*(4), 333–369. https://doi.org/10.1016/S0364-0213(81)80017-1

MITRE. (2012). Cyber Resiliency Metrics. In *MITRE Report MP 120053 Rev 1*. (Issue April). https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity v 1.1. In *National Institute of Standards and Technology*. https://doi.org/10.1109/JPROC.2011.2165269

Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E., and Simonsen, S. (2019). A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grids. *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, *June*, 39–51. https://doi.org/10.5220/0007697800390051

Pham, C., Tang, D., Chinen, K., and Beuran, R. (2016). CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. *Proceedings of the Seventh Symposium on Information and Communication Technology*, 251–258. https://doi.org/10.1145/3011077.3011087

Richardson, G. P., and Pugh, A. L. (1981). *Introduction to System Dynamics Modeling*. Pegasus Communications. https://books.google.es/books?id=lqwvAAAACAAJ

Sitzmann, T. (2011). A meta-analytic examination of the instructional effectiveness of computer-based simulation games. *Personnel Psychology*, *64*(2), 489–528. https://doi.org/10.1111/j.1744-6570.2011.01190.x

World Economic Forum. (2020). *The Global Risks Report 2020*. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf