The Dynamics of Cyber Resilience Management

Juan Francisco Carías
University of Navarra, TECNUN, School of Engineering, San Sebastian, Spain
jfcarias@tecnun.es

Leire Labaka
University of Navarra, TECNUN, School of Engineering, San Sebastian, Spain
llabaka@tecnun.es

José María Sarriegi
University of Navarra, TECNUN, School of Engineering, San Sebastian, Spain
jmsarriegi@tecnun.es

Andrea Tapia
Pennsylvania State University, USA
axh50@psu.edu

Josune Hernantes
University of Navarra, TECNUN, School of Engineering, San Sebastian, Spain
jhernantes@tecnun.es

ABSTRACT

With the latent problem of security breaches, denial of service attacks, other types of cybercrime, and cyber incidents in general, the correct management of cyber resilience in critical infrastructures has become a high priority. However, the very nature of cyber resilience, requires managing variables whose effects are hard to predict, and that could potentially be expensive. This makes the management of cyber resilience in critical infrastructures a substantially hard task.

To address the unpredictability of the variables involved in managing cyber resilience, we have developed a system dynamics model that represents the theoretical behaviors of variables involved in the management of cyber resilience. With this model, we have simulated different scenarios that show how the dynamics of different variables act, and to show how the system would react to different inputs.

Keywords

Cyber resilience, System dynamics, Critical infrastructure protection (CIP).

INTRODUCTION

Society's welfare is dependent on the effective performance of Critical Infrastructures (CIs) to provide our energy, water supply, transportation, sanitation and telecommunications (National Research Council (U.S.), 2009). CIs are defined as systems, services and assets that are vital for the welfare of society, and whose disruption or destruction has severe impact on the health, security, safety or economic well-being of citizens and on the effective functioning of government (Commission of the European Communities, 2005). Natural disasters, terrorist attacks and cyber incidents are the main threats to which CIs are exposed to. Actually, the latter are considered by the World Economic Forum as one of the most likely global risks, with high impact in case of occurring (World Economic Forum, 2018).

The cyber-attack on a power grid occurred in 2015 in Ukraine is an example of the impact of these threats. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. Thirty substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours. First, the hackers compromised the network using spear-phishing emails with the BlackEnergy malware. Then, they seized control of the SCADA system, which let them switch substations off remotely, disable the IT infrastructure components and destroy files

with the KillDisk malware. Finally, they carried out a denial of service attack against the company's call center to deny consumers up-to-date information on the blackout (Lee *et al.*, 2016).

Furthermore, CIs have grown in size, complexity and interconnectivity to guarantee a high level of reliability and safety in their services, but in doing so they have also increased their vulnerability, providing more surface areas for criminal hackers to exploit. Moreover, the perspective for the next years is not satisfactory, since it is expected that the number of cyber-attacks will continue increasing causing a significant negative effect on countries and industries (ENISA, 2016). Besides, the problem could be analyzed from the all hazards approach and not limit the cyber crises to cyber-attacks. Instead, considering that cyber incidents could be "acts of God" (for example, natural disasters that compromise the systems) or "acts of man" (that could be unintentional or intentional) (Björk *et al.*, 2015), the cause of cyber incidents could be black-boxed and have a broad spectrum of threats to the functionality of the CI's systems. This context has led to increasing concern about the reliability and security level of CIs, making the creation of resilient CIs that are able to cope with crises an issue of paramount importance (Federal Register, 2015).

In the last years, there has been an evolution in the approach to address the cyber threats. The cyber security approach, which focused on protection strategies, has evolved to a more strategic and long term thinking approach called cyber resilience (World Economic Forum, 2017). Cyber resilience is defined as the "ability to withstand and recover quickly from unknown and known threats" (Linkov *et al.*, 2013). To deal with future cyber incidents it is vital to integrate physical and cyber management, strengthen resilience leadership and organizational processes, and leverage supporting technologies (World Economic Forum, 2017). In this context, cyber resilience provides a holistic approach that focuses on systems rather than individual organizations (Kaplan *et al.*, 2015).

In this paper, we present a System Dynamics model that includes the policies identified by the frameworks in the literature. This model aims to increase CI providers' awareness about the importance of investing on cyber resilience policies considering a holistic approach. This simulation model aims to show the relationships between the technical, social and regulatory factors in the cyber resilience building process that have been identified in these frameworks. The aggregated perspective of the problem given by an SD model can help security managers to design and implement more effective policies, seeking a compromise among different investment strategies such as technology, training, learning, collaboration and legal requirements.

LITERATURE REVIEW

Several frameworks can be found in the literature that define a set of characteristics, stages and policies to develop and assess cyber resilience in organizations. For example, Linkov et al. (2013) defines a matrix that helps organizations to manage adverse events. This matrix combines four domains (physical, information, cognitive and social) with four stages that define the event management cycle that a system needs to follow to be resilient: plan and prepare, absorb, recover and adapt. Thus, each cell in the matrix contains policies or actions that address the question: ''How is the system's ability to [plan/prepare for, absorb, recover from and adapt to] a cyber-disruption implemented in the [physical, information, cognitive, social] domain?''.

The National Institute of Standards and Technology (NIST) develops a Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018), that defines five stages, called functions, in the cybersecurity management lifecycle: 1) identify (develop understanding of and manage risk to systems, assets, data, and capabilities), 2) protect (develop and implement appropriate safeguards to ensure delivery of critical infrastructure services), 3) detect (identify the occurrence of a cybersecurity event), 4) respond (take actions regarding a detected cybersecurity event), and 5) recover (maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event). Each of these stages or functions are subdivided in categories and subcategories, that provide aspects to consider for cyber resilience building process. This framework has 22 categories divided into 98 subcategories. For example, the category "Asset Management" is divided into subcategories like "Physical devices and systems within the organization are inventoried", "Software platforms and applications within the organization are inventoried", etc. (NIST, 2018).

On the other hand, World Economic Forum develops its own framework combining the characteristics of frameworks developed by NIST and Linkov (World Economic Forum, 2016a). This framework uses the four domains defined by Linkov and a combination of stages defined in the two previous frameworks. The stages are: 1) Plan and prepare 2) detect, 3) absorb, 4) recover and 5) adapt. Each cell of this framework includes several policies to build the cyber resilience of the organization. For example, in the physical domain, for the plan and prepare stage, there are policies such as: "Implement controls/sensors for critical assets" or "Assessment of network structure and interconnection to system components and to the environment" (World Economic Forum, 2016a).

The described frameworks suggest the implementation of dozens of policies to build cyber resilience. Investments

are needed to develop these policies but some-times it is hard to understand and measure the impact of these policies in the cyber resilience enhancement in the short, medium and long term. Simulation models can help understand the effects of different policies over time under different conditions or scenarios. Actually, simulation models can represent the real system in a mathematically reliable way simulating the behavior of complex systems over time, enabling users to understand, train and learn about how the complex a system works (Coll, Richard & Lajium, 2011).

System Dynamics (SD) is a modeling and simulation methodology that has been used in several disciplines of research such as in engineering, scientific humanitarian sciences, economy, manufacturing and management, planning and logistics, healthcare, urban planning etc. The SD uses a top-down approach that allows to manage and analyze complex adaptive systems involving interdependencies (Forrester, 1961; Sterman, 2000). This methodology is grounded in the theory of nonlinear dynamics and feed-back control, which deals with the internal feedback loops and time delays that influence the whole system (Casalicchio *et al.*, 2007).

SD methodology allows modelling effectively socio-technical systems, consisting of human, organizational and technological parts. In particular, SD is used when the individual properties are not decisive and high-level aggregation is desired or required for management purposes. This is typically the case for management strategies and long-term planning (Iturriza *et al.*, 2018; Sarriegi *et al.*, 2008).

SD's top-down approach and its high-level aggregation allow this modeling and simulation technique to include "soft" variables whose dimensions are usually unknown and their values difficult to measure exactly (Forrester, 1980; Labaka *et al.*, 2015). This is possible because SD's approach considers high level causal relationships and the general structure of the system and not the specific values of variables (Forrester, 1980). Moreover, these variables', even though they have unknown values, cannot be left out of the model since that would be to consider they have no effect, but most of the time the effect of soft variables such "morale", "awareness" or "commitment" are known to have crucial effects on many socio-technical systems (Forrester, 1980).

These characteristics are known to be part of the cyber resilience management and building processes. On the one hand, cyber resilience development involves complex and multiple relations between variables and the presence of significant delays. The process of building cyber resilience in an organization needs to consider variables that evolve quickly, like new type of cyber-attacks or software upgrades, with others that need longer times to change, such as organizational culture or individual attitudes towards security. On the other hand, building cyber resilience involves soft variables that cannot be directly measured, such as employees' awareness, cyber resilience level, etc., but that have crucial effects on the evolution of cyber resilience management. And for these reasons, we consider that SD is especially suitable to model and simulate cyber resilience management.

Besides, through the simulation of different scenarios in an SD model, managers can determine the investment strategy that best suits their objectives and needs since they can see what the results of their investment strategies would be according to the structure of the system that has been modeled. This does not mean that the model is predictive, but that a model that follows the theoretical behaviors can give managers some awareness of what the consequences of their investment decisions are.

SYSTEM DYNAMICS MODEL

In this paper we have developed a System Dynamics (SD) model that allows CIs providers (independently of whether their private or public) to reflect on the consequences of adopting different policies to improve the cyber resilience level. The developed simulation model includes what the literature identifies as key aspects and policies to build cyber resilience and models their interrelationships. This makes the model a useful tool for exploring different scenarios to see how the implementation of some policies or lack thereof can affect the impact of cyber incidents in a critical infrastructure over time.

Due to the nature of SD, the models developed with this technique can be summarized in causal loop diagrams (CLD). CLD represent causal relationships, causal loops and interactions between causal loops through variables and arrows. In a CLD an arrow represents a causal relationship, and the "polarity" of the causal relationship is depicted as a + or – sign near the head of the arrow. In this sense, the + sign represents a directly proportional relationship (i.e. when the variable near the base of the arrow increases, the variable near the head of the arrow increases as well and vice versa), and the – sign represents inversely proportional causal relationships (i.e. when the variable near the base of the arrow increases, the variable near the head of the arrow decreases and vice versa).

As said previously, cyber resilience provides a holistic approach that focuses on systems rather than individual organizations (Björk *et al.*, 2015). This means that CI's internal and external aspects should be taken into account (Labaka *et al.*, 2013). The developed model includes both aspects/contexts: internal and external that are explained in the following sub-sections.

Internal Cyber Resilience Sub-Model

The internal cyber resilience sub-model is limited to the CI boundaries. This sub-model represents policies such as investments in technology, training, systematization and learning that are influenced by the level of awareness of decision makers. All these policies can be found in different frameworks and standards in the literature (Linkov *et al.*, 2013; NIST, 2018; World Economic Forum, 2016b).

The policies included in this sub model and their behavior are described as follows:

- Awareness represents the level of knowledge the decision makers of the CI has about the vulnerabilities and risks that surround that organization. Awareness level triggers the investments in Training, Cybersecurity equipment or both. This causal relationship is represented with causal loop notation in Figure 1.

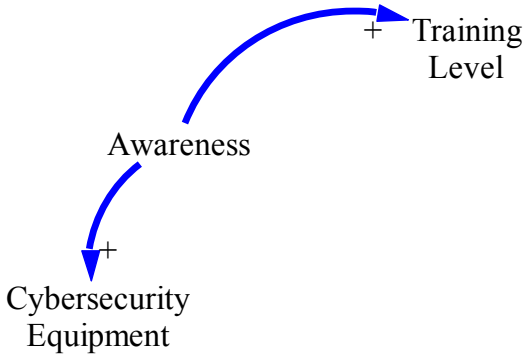


Figure 1 Relationship between Awareness, Training Level and Cybersecurity Equipment

- When the organization invests in Training the staff learns about the risks that surround the organization and the best practices currently available in order to mitigate them. Hence, the level of Training will also increase the Awareness, because as the staff gets to know more, they will be more concerned about how vulnerable the organization is because of their lack of knowledge. This added relationship can be depicted as in Figure 2.

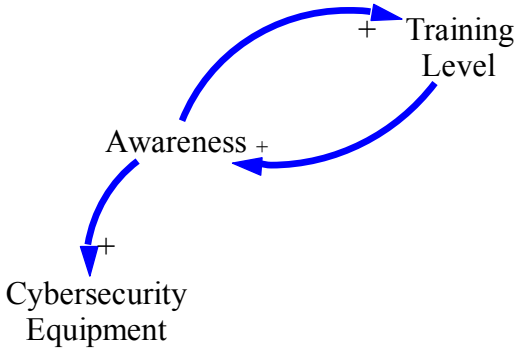


Figure 2 Training Level has a directly proportional relationship with awareness

- Systematization is the policy where internal standard processes are created to prevent incidents, mitigate them and recover from them. This policy is a direct effect of the Training policy and will only start to be applied when the staff has a certain Training level where they are able to design efficient processes. This new variable would be related to the previous ones as shown in Figure 3.

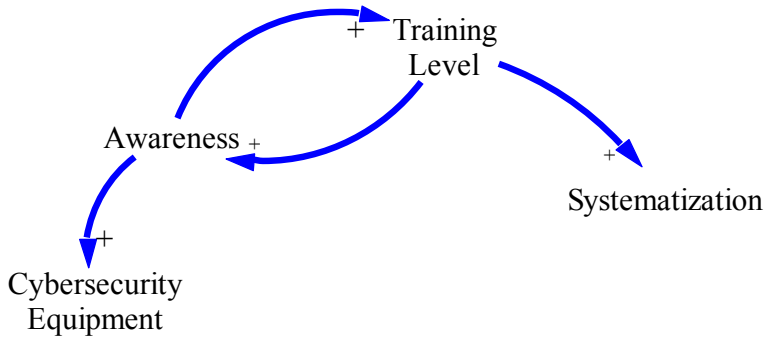


Figure 3 Trained staff can start developing systematic cyber resilience processes

- The model also takes into account the investment on Cybersecurity equipment policy. This policy represents the acquisition of software for protection against threats and detection of cybersecurity incidents.
- When the organization suffers a disruption because of an Impact event (when it has an Impact > 0) the organization's Awareness level increases. This can be represented as in Figure 4.

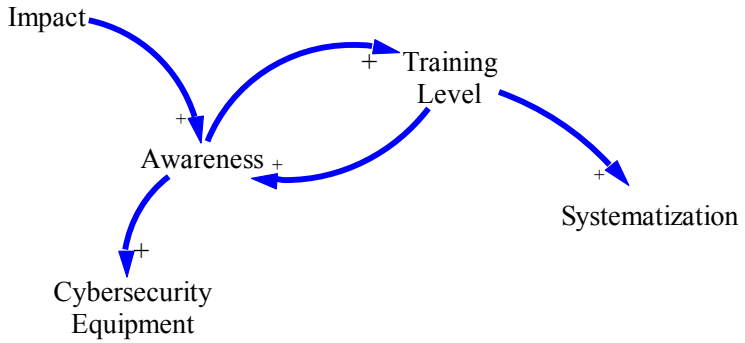


Figure 4 Impacts to the company increase awareness

In order to represent how these policies affect cyber resilience level when implemented or not implemented, they are related to the variables *Prevention capacity*, *Absorption and recovery capacity* or both. *Cybersecurity equipment* is considered to have no effect on the *Absorption and recovery*, but to have great impact on the *Prevention capacity* because most commercial software is designed to protect, and when a system is infected, protective software does not help to mitigate the crisis. On the other hand, *Training* and *Systematization* help both *Prevention* and *Absorption and recovery capacity* since knowledge of the threats, and standard processes can help the personnel recover faster from a crisis. Also, to complete the representation of the cyber resilience management, the *Internal lessons learned* variable is a representation of the adaptation stage of cyber resilience, that according to Linkov et al. is "Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient" (Linkov *et al.*, 2013). With these added relationships, the model has all the relationships shown in Figure 5.

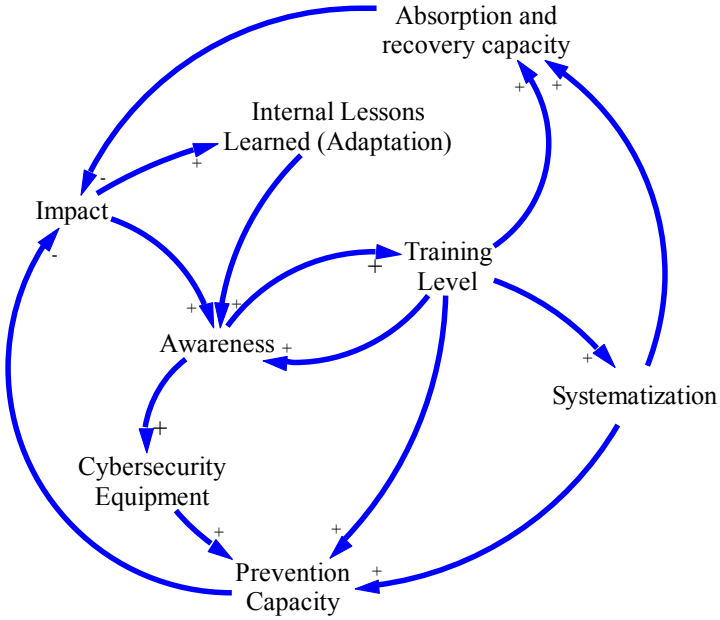


Figure 5 Relationships in the internal cyber resilience sub-model

In turn, Prevention capacity and Absorption and recovery capacity, affect the Impact inflow and outflow in the following way:

- A higher *Prevention capacity* would decrease the magnitude of the impact making the *Impact increase* be lower for any *Impact event* and as a consequence resulting in a lower value for the *Impact* stock, and vice versa.
- A higher *Absorption and recovery capacity* would decrease the recovery time making the *Impact decrease* higher, resulting in a lower value for the *Impact* stock, and vice versa.

External Cyber Resilience Sub-Model

In order to capture the effect of the external context in the cyber resilience of an organization, we have made a second sub-model that includes policies from the literature such as:

1. Collaboration: it represents how through a Collaboration policy an organization is able to learn from cybersecurity incidents that have not yet happened to them but have happened to other organizations.
2. Regulation: this sub-model represents how even if the organization does not invest in Collaboration and therefore does not learn from external cybersecurity incidents, high impact cyber events can foster the tightening of legal requirements. This tightening in legal requirements would make the organization more aware of the risks in the environment, and thus more investment on cyber resilience policies would be applied.

The behavior of this sub model is described as follows:

- External Impact is a variable that represents the incidents suffered by other organizations.
- Collaboration represents how much communication the organization has with external stakeholders and surrounding organizations. Thus, when there is no Collaboration, no matter how the External impact variable behaves, there will be no External lessons learned. On the other hand, the more Collaboration there is, the more External lessons learned increases when surrounding organizations suffer incidents. When the organization learns from what happened to other organizations, the Awareness increases as well, because the decision makers would become aware of the surrounding risks. This can be represented in CLD notation as shown in Figure 6.

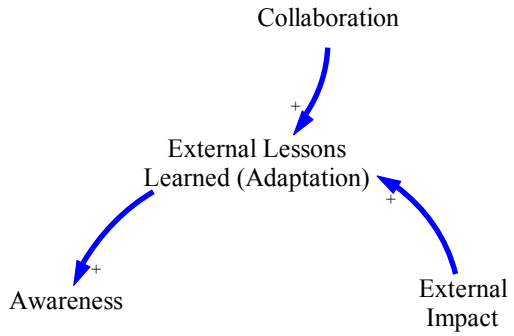


Figure 6 The lessons learned from incidents to other companies depend on the level of collaboration

- Independently of how much Collaboration there is, External Impact affects the legislation: the bigger the impact on other critical infrastructures, the more New legal requirements will appear. These New legal requirements that the organization needs to comply with, make the decision makers aware of what happens outside of the organization increasing their level of Awareness. This is the final relationship in the external cyber resilience submodel and can be represented as in Figure 7.

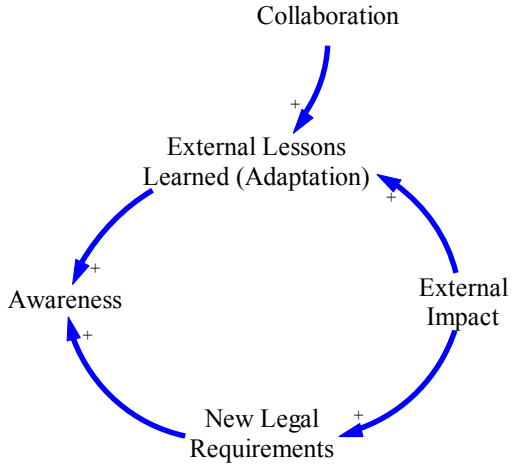


Figure 7 All the relationships in the external cyber resilience sub-model

This sub-model is connected to the internal cyber resilience sub-model because the policy of Collaboration affects the Absorption and recovery capacity, and because New legal requirements will appear when significant cybersecurity crises happen either to the organization or to external organizations. Also notice that by joining these two sub-models it is possible to model the complete cyber resilience management of a critical infrastructure.

SIMULATIONS

The effect of different policies included in the simulation model has been analyzed in the different scenarios shown in Table 1.

Table 1 Simulation Scenarios

Group	Scenario
Internal Crises	Series of internal crises Series of internal crises with no investment on training Series of internal crises with no investment on cybersecurity equipment
External crises	Series of external crises Series of external crises with no investment on collaboration
External and internal crises	Series of external and internal crises

Internal Crises Scenarios

The internal crises scenarios assume that nothing happens to external organizations and the organization being studied suffers three big crises at months 10, 50, and 90. The scenarios simulated in this model assume that there is a limited budget that can be either invested on training or on cybersecurity equipment, however, since every CI has a different budget and since when using SD the specific values of variables are not as important as the general structure of the system, this budget has been assigned through percentages. In this sense, the three internal crises scenarios that have been simulated demonstrate the behavior of the model on the following three cases:

1. A base run, where the organization invests on training and on cybersecurity equipment equally (50%-50%) according to its awareness level. This case is called Series of Internal Crises.
2. A second scenario where the organization does not invest on cybersecurity equipment, but invests 100% of its budget on training and collaboration. This case is called Series of Internal Crises with no Investment on Cybersecurity Equipment.
3. A third scenario where the organization does not invest on training, but invests 100% on cybersecurity equipment and collaboration. This case is called Series of Internal Crises with no Investment on Training.

The simulation of these scenarios shows that in the case of internal cyber resilience, investing only on training is more sustainable than investing only on cybersecurity equipment. This can be supported by comparing Impact graph on the three scenarios (see. Figure 8). On this graph, the base run shows a decreasing trend, while Series of Internal Crises with no Investment on Training run shows not only a bigger Impact with every crisis, but also with each crisis it takes longer to recover. These behaviors are due to the effect of not having Training and Systematization on the Prevention capacity and the Absorption and recovery capacity. On the other hand, not having cybersecurity equipment, makes the Impact grow at the beginning, but on the long-term the impact ends up decreasing with respect of the initial crisis.

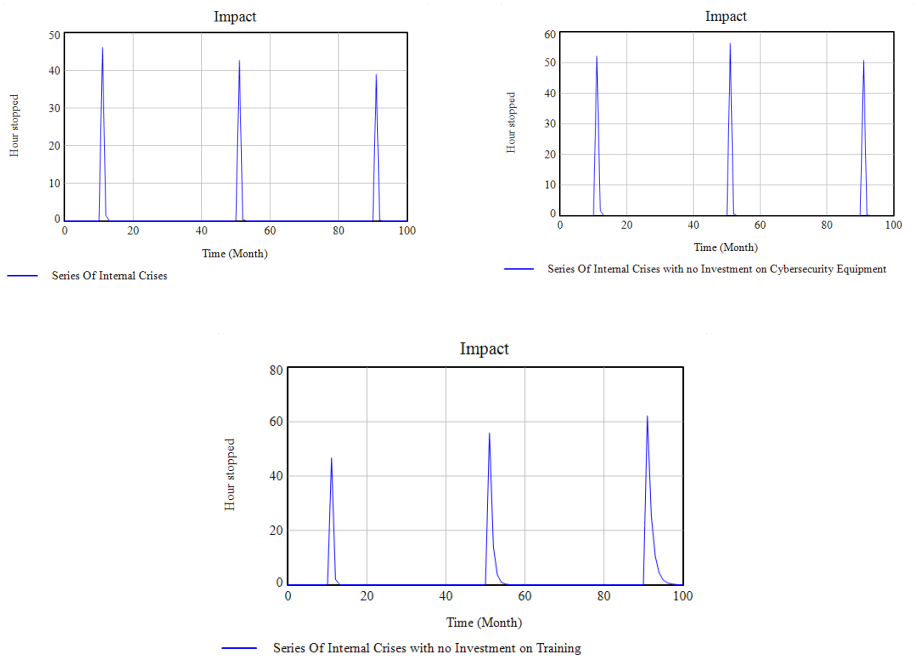


Figure 8 Impact behavior in internal crises scenarios

Another way of supporting that a training policy is of critical importance in a CI is the Awareness variable's behavior over time (see. Figure 9). This graph shows how, when not investing on training, Awareness only grows when there is a crisis and it grows because of the new legal requirements that appear and because of the lessons that are learned from the suffered impact. However, the lack awareness due to the lack of knowledge of the surrounding risks makes this kind of Awareness unsustainable, and thus the Awareness variable's trend is to decrease.

On the other hand, when there is no investment on cybersecurity equipment, due to the higher investment in training, the awareness reaches higher levels than on the base run. The reason behind this behavior is that the investment in training reinforces the management's knowledge of the risks to the CI and knowing more about the threats that the company is exposed to makes the management more aware of the problems the company may have. This behavior is also comprehensible since having more impact in the short-term would worry the

management more and thus make them more aware from the beginning.

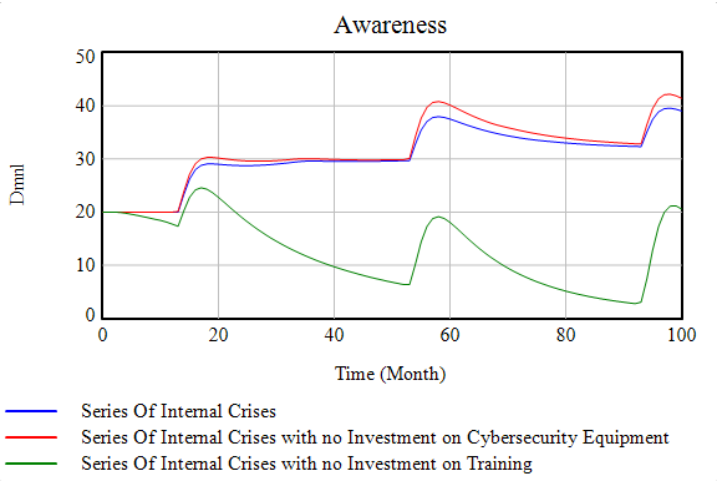


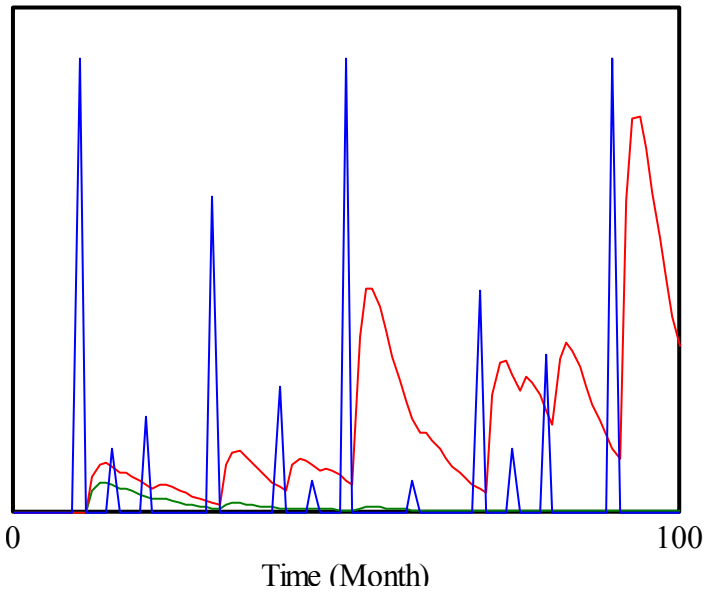
Figure 9 Awareness behavior in internal crises scenarios

External Crises Scenarios

The external crises scenario group assumes that nothing happens inside the organization but the external organizations are suffering different-sized cyber incidents over time. The two scenarios simulated demonstrate the behavior of the model on the following two cases:

1. A base run, where the organization invests in all possible policies, including Collaboration. This scenario is called Series of External Crises.
2. A second scenario where there is no investment on Collaboration, but the organization does invest in training, and cybersecurity equipment. This scenario is called Series of External Crises with no Investment on Collaboration.

The purpose of these scenarios is to show the benefits that Collaboration has on the organization's cyber resilience. These benefits can be shown by comparing the crises that external organizations have suffered and the External lessons learned that the organization acquires from those crises (see Figure 10). On both scenarios the External impacts are the same. The graph shows that, as explained when describing the model, when there is no Collaboration, no matter how the External impact varies, the organization does not learn from what happens to others. On the graph, this behavior is shown as well as an increasing learning with each crisis on the Series of External Crises case where there is investment on Collaboration.



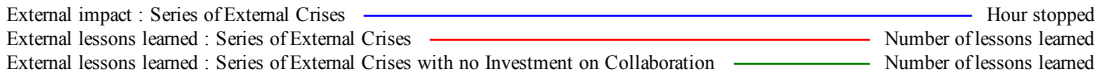


Figure 10 External impact and external lessons learned in external crises scenarios

Another result of investing on Collaboration can be observed on the behavior over time of the Awareness variable (see Figure 11). On this graph the effect of Collaboration is shown with higher values on the Awareness variable for the case where there is Collaboration. Another effect of Collaboration besides this increasing difference between the case with no Collaboration and the base case, is the increasing peaks of Awareness on crises that are a direct result of the External lessons learned that have been shown before.

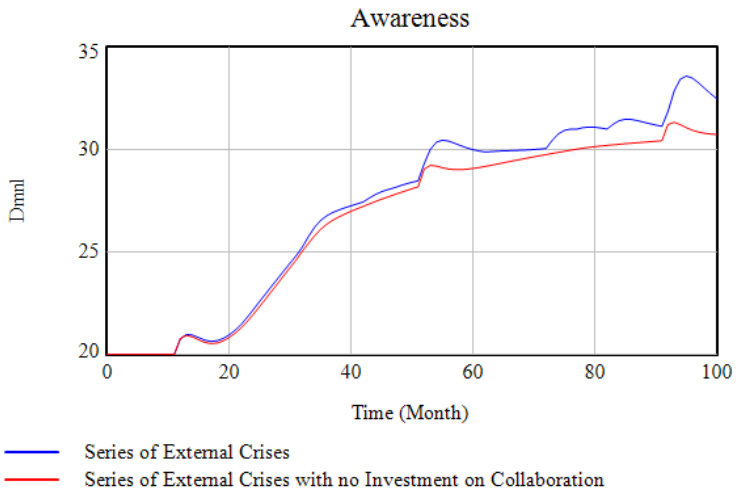


Figure 11 Awareness behavior in external crises scenarios

Internal and External Crises Scenario

Finally, the internal and external crises scenario shows how the organization would behave when there are different-sized external crises and a series of internal crises over time. To do this, the input crises for both of the previous groups have been applied. This scenario demonstrates the normal operation of the organization when it applies all of the policies that have been modelled.

As expected, the impact caused by the crises the organization suffers over time has a decreasing trend, just as it had when the *Series of Internal crises* scenario was simulated (see Figure 12). However, this time the decreasing trend is slightly steeper because of the effect of *Collaboration* on the *Awareness* of the organization. Also, in this scenario, the time to absorb and recover from the impact is also slightly smaller because of the effect of *Collaboration* on the *Absorption and recovery capacity* of the organization.

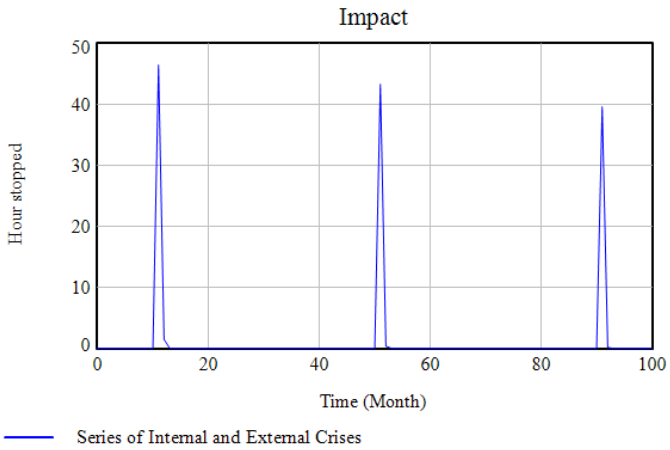


Figure 12 Impact on Internal and External crises scenario

Notice that this final scenario's behavior over time will be the sum of the base run scenarios' behaviors over time on the previous groups. This can be observed, for example, on the behavior over time graphs of the *Awareness* of

the two previous groups' base cases and the *Awareness* on the *Series of Internal and External Crises* scenario (see Figure 13). This graph shows how internal crises affect *Awareness* significantly more than external crises, and that investing on all cyber resilience policies that have been modelled when the organization is in an environment where there are internal and external crises result on more *Awareness.* This increase in Awareness, would in turn result on a better cyber resilience because of the causal relationships inside the model.

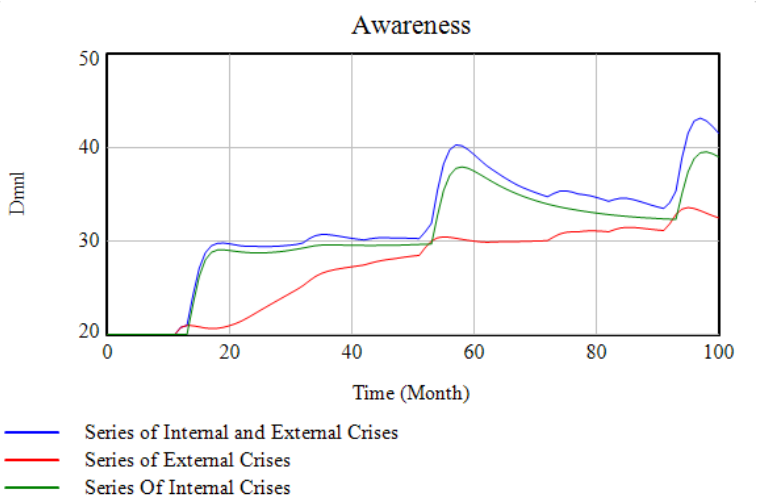


Figure 13 Awareness on the base run of the three scenario groups

CONCLUSIONS AND FUTURE RESEARCH

In this paper, we have developed an SD model that gives some insight on the management of cyber resilience on a critical infrastructure. To do this, theoretical relationships between variables related to cyber resilience have been modeled. These variables and relationships include cyber resilience domains as well as policies.

Through this model and through simulations done on it, the following conclusions have been drawn:

- When speaking about internal cyber resilience, investing only on cyber security equipment (state of the art software to protect the organization from cyber events) is a short sighted strategy that will end up having repercussion in the CI. On the other hand, investing only on training is more viable in the long term, but not ideal since it leaves the CI unprotected in the short-term.
- Collaboration with external organizations has slow results, but it adds up to help significantly to increase the Awareness as well as the Absorption and recovery capacity of the organization.
- For an optimal management of an organizations cyber resilience it is necessary to apply both, internal and external policies in the organizations resilience management plan.

The model described on this paper, however, has limitations as it is merely demonstrative and only reflects the theoretical behaviors of an organization applying these policies. Reality is much more complex and more variables are involved. This model should be validated with experts' knowledge and its limitations should be addressed in future research through the calibration of the model with real organizations' data such as a real budget and a real investment plan.

ACKNOWLEDGMENTS

The authors thank the support from the Basque Government project ELKARTEK 2017 KK-2017/00044 and project ELKARTEK 2018 KK-2018/00076.

REFERENCES

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

Casalicchio, E., Galli, E., & Tucci, S. (2007) Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures In: *11th IEEE International Symposium on Distributed*

Simulation and Real-Time Applications (DS-RT'07) pp. 182–189. doi:10.1109/DS-RT.2007.11

Coll, Richard, K. & Lajium, D. (2011) *Modeling and the future of science learning Models and Modeling: Cognitive Tools for Scientific Enquiry*. doi:10.1007/978-94-007-0449-7

Commission of the European Communities (2005) COM(2005) 576: Green Paper on a European Programme for Critical Infrastructure Protection, 1–26.

ENISA (2016) *The cost of incidents affecting CIIs*.

Federal Register (2015) L2: Executive Order 13636: Improving Critical Infrastructure Cybersecurity.

Forrester, J. W. (1961) *Industrial dynamics*. MIT Press, Cambridge, MA.

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

Iturriza, M., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018) Modelling methodologies for analysing critical infrastructures *Journal of Simulation*, **0**, 1–16. doi:10.1080/17477778.2017.1418640

Kaplan, J. M., Bailey, T., Rezek, C., O'Halloran, D., & Marcus, A. (2015) *Beyond Cybersecurity: Protecting Your Digital Business*. John Wiley & Sons (US). Retrieved from https://books.google.es/books?id=hCisBwAAQBAJ

Labaka, L., Hernantes, J., Rich, E., & Sarriegi, J. M. (2013) Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery *Journal of Homeland Security and Emergency Management*, **10**, 289–317.

Labaka, L., Qian, Y., Lango, P., & Gonzalez, J. J. (2015) Insights from a computer simulation model of a landslide disaster *Proceedings of the Annual Hawaii International Conference on System Sciences*, **2015**–**March**, 192–199. doi:10.1109/HICSS.2015.32

Lee, R. M., Assante, M. J., & Conway, T. (2016) Analysis of the cyber attack on the Ukrainian power grid *SANS Industrial Control Systems*, 23.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013) Resilience metrics for cyber systems *Environment Systems and Decisions*, **33**, 471–476. doi:10.1007/s10669-013-9485-y

National Research Council (U.S.) (2009) *Sustainable critical infrastructure systems : a framework for meeting 21st century imperatives : report of a workshop*. National Academies Press.

NIST (2018) *Framework for Improving Critical Infrastructure Cybersecurity National Institute of Standards and Technology*. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Sarriegi, J. M., Sveen, F. O., Torres, J. M., & Gonzalez, J. J. (2008) Adaptation of Modelling Paradigms to the CIs Interdependencies Problem In: *Critical Information Infrastructure Security CRITIS* pp. 295–301.

Sterman, J. D. (2000) *Business dynamics: Systems thinking and modeling for a complex world*. Irwin/McGraw-Hill, Boston.

World Economic Forum (2016a) *A framework for assessing cyber resilience*. Retrieved from http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf

World Economic Forum (2016b) A framework for assessing cyber resilience.

World Economic Forum (2017) *Advancing Cyber Resilience - Principles and Tools for Boards*. Retrieved from http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

World Economic Forum (2018) *The global risks report 2018, 13th edition*. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf%0Ahttp://www3.weforum.org/docs/WEF_GRR18_Report.pdf%0Ahttps://www.weforum.org/reports/the-global-risks-report-2018