A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks

Miguel Hernández-Bejarano*, Ricardo J. Rodríguez†, José Merseguer†
*Fundación Universitaria Los Libertadores (FULL), Bogotá, Colombia
mhernandezb@libertadores.edu.co
†Universidad de Zaragoza, Spain
{rjrodriguez, jmerse}@unizar.es

***Abstract*—Nowadays, business organizations support daily operations using Information and Communication Technologies. They serve as a basis to have a controlled management of resources, services and business goals, aligned with the mission of the organization. In this paper, we review standards and frameworks for achieving cyber-resilience in organizations, such as the NIST framework, ENISA, or international standards as the ISO/IEC 27032. We then envision the need of a new cyber-resilience framework that leveraging machine learning techniques contributes to improve business continuity.**

***Index Terms*—Cybersecurity, resilience, menaces, vulnerabilities, cyber-attacks**

I. Introduction

Human and technological menaces compromise governmental and non-governmental organizations alike. These menaces focus on leveraging software and hardware vulnerabilities [1] for carrying out complex cyberattacks, such as the recent ransomware attacks of WannaCry or NotPetya, to name a few. Consequently, organizations are continuously developing and deploying policies and technologies to protect their systems. Nowadays, most of the organizations handle information that if correctly managed may represent their most important asset. In this regard, information is understood as the set of data, already processed and classified, which is suitable for creating knowledge, making decisions, and choosing alternatives. In addition, useful information needs to be continuously trusted and updated, so to serve timely and adequately to its purposes. Thus, companies need to understand that a correct information assurance heavily relies on protection and availability of their data [2].

Resilience is defined as the ability for a system, or even for a company, to recover and quickly adapt from undesired events [2], [3]. Such ability helps to tackle uncertainties in daily operations, as well as to manage inherent complexities of companies. Resilience may also help overcome failures menacing the core of the company operation. In this regard, it is needed a collective consciousness engaging people, organizations and governments to improve as much as possible the protection levels. However, inconsistencies in applying, measuring and assessing resilience in the business environment are often found in practice. Thus, benefits are rarely obtained. The Organization for Economic Co-operation and Development is particularly concerned with applying resilience principles to information systems globally to alleviate menaces focused on economical aspects and social development.

Like in many other fields, cyber-resilience refers to the system's ability to recover its normal behavior, thus overcoming performance degradations, after a cyberattack [4]. Therefore, cyber-resilience becomes a critical means in the practice of cybersecurity, especially for critical infrastructures. A resilient system, company, or infrastructure successfully and holistically aligns service continuity and errors recovery with daily security practices. Resilience is then key for preserving system functionalities, while mitigating the consequences of undesired menacing events [5]. Resilience measures system trust and is understood as a cyclic process, based on continuous improvement, for preventing, absorbing, recovering, and adapting the system or critical infrastructure before emergencies.

In this regard, cybersecurity frameworks, standards and good practices contribute to understanding the different types of attacks and to manage cyberattacks [6]. For instance, the National Institute of Standards and Technology (NIST) provides a simple and effective framework that supports five risk management functions: identify, protect, detect, respond, and recover. In order to provide current and future cybersecurity to organizations, the NIST framework also aligns with the NIST guidelines and recommended good practices [7], [8].

On the other hand, advances in communication technologies and hyper-connectivity facilitate the access and exchange of information to organizations of any size and sector. Likewise, cyberattacks are increasingly sophisticated and innovative. Their inevitability, coupled with the continued growth of criminal sophistication, push organizations toward cyber-resilience. From this point of view and considering the need of continuity for system activities, we envision to incorporate machine learning

The research of R. J. Rodríguez and J. Merseguer was supported in part by the University, Industry and Innovation Department of the Aragonese Government under *Programa de Proyectos Estratégicos de Grupos de Investigación* (ref. T21-17R) and by the University of Zaragoza and the *Fundación Ibercaja* under grant JIUZ-2020-TIC-08.

algorithms as an integration between cybersecurity and cyber-resilience. In our research context, machine learning is used as a tool for predicting threats and analyzing potential exploitable flaws. Machine learning can then significantly improve the effectiveness of security controls, as it can also provide a more complete information on the actions of cyber-attackers to facilitate a timely response before any incidents happen.

In this paper, we settle the basis of our next research. We aim to leverage machine learning techniques for improving business continuity, by learning from current cybersecurity frameworks.This paper is organized as follows. Section II gives the background and motivation. Section III revises important frameworks that offer concepts to support our expected achievements. Section IV details our proposed solution methodology. Finally, Section V envisions the future directions of our research.

II. Background and Motivation

Cyberattacks have increased in sophistication, impact, and scope during the last decade, exposing organizations to large data breaches that not only incur in direct financial losses, but also in other damages such as brand reputation and legal consequences. For instance, the General Data Protection Regulation, which applies directly in the UE and indirectly to any organization handling data of European citizens, imposes fines of millions of euros due to security breaches that expose personal data [9]. Therefore, cybersecurity risk policies and incident response plans help reduce the risk exposure to be attacked and minimize the potential impact of a successful attack.

Organizations must interrupt their daily operations while their system capacities are degraded due to the presence of cyberattacks. To defend and protect network assets, some organizations improve their perimeter security (extending it with firewalls and intrusion detection systems, for instance), while others invest in incident response processes [10]. However, as the Internet was originally created for research and not for commercial use, security was then not taken into account in its design [11]. According to the Internet Crime Report 2017 [12], the Internet Crime Complaint Center under the Federal Bureau of Investigation received 301,580 complaints with an estimated loss of $1,418 million. As a matter of fact, insurance companies now offer their customers special insurances to cover cybersecurity incidents [13].

Cybercriminals are always taking advantage of undergoing crisis. For instance, from February to April 2020, during the rise of COVID-19, cyberattacks against the financial sector increased by almost 238% [14]. A McAfee report presents that the threats related to COVID-19 have been really important and decoys have been used in all kinds of attacks. McAfee observed 375 threats per minute in Q1 2020, reporting about malicious detections in almost every country affected by the COVID-19 pandemic [15].

These issues put in evidence that cybersecurity is a priority for state politics and needs to be taken into account in a holistic way, considering economic, educational, legal, technical, and sovereignty aspects. Recall that a system perfectly secure does not exist, and thus, it is just a matter of time to be the target of attackers. Cybersecurity technologies, policies, and regulations need to be developed to prevent these issues [16].

III. Current Frameworks for Cyber-Resilience

The need for organizations to consciously protect the valuable resource of information from cyberattacks has developed the concept of *organizational resilience*. This means tracking, protecting and defending the assets that collect logs and the systems that track the devices [17]. For this reason, organizations in any productive sector can be subjected to tensions, caused by cybersecurity incidents generated in their environment, both internal and external. In this sense, cybersecurity frameworks, maturity models and standards, provide the ability for the organization to identify and protect its critical systems from evolving cyberthreats, while detecting cyber intrusions that could cause interruptions in operations [1]. Additionally, organizations must be equipped with capabilities to respond to and recover from a critical cyber event. Taking into account that a cybersecurity framework is a system of standards and good practices, it can be used as a tool to manage cyber-attacks, also for a better understanding of the different types of attacks and, in turn, for the recovery of a system resulting from an attack [1]. On the other hand, a security framework should support a standard-based model into which custom plugging extensions can be integrated to improve security functionality and data entry validation [18].

In the following, we review some of the important cybersecurity frameworks that can help to manage business continuity, in order to avoid the interruption of the vital services of an organization and to restore full operation, as quickly and easily as possible. They are summarized in Table I. The NIST framework [8] is a tool for the management of cybersecurity risks, which motivates technological innovation and adapts to any type of organization. This framework groups cybersecurity activities into five functionalities: identify, protect, detect, respond and recover. It is one of the most used standards for developing cybersecurity methodologies, it establishes how to guide the development of cyber-resilience infrastructure and therefore help to maintain a secure environment. The ISO 27000 [19] is a family of standards, geared towards information security issues, helping organizations to maintain and manage the security of assets such as financial information, intellectual property or information of employees. Additionally, ISO 22301 [20] enables an organization to identify threats relevant to its business and critical business functions that could be affected. Fundamentally, it enables the organization to define and

establish plans in place, in advance to ensure business continuity. Other organizations or entities, such as ENISA [21] help EU countries to be better prepared to prevent, detect and respond to information security problems in case of attacks.

These internationally recognized standards help to raise the levels of quality, safety, reliability, efficiency and interchangeability. The NIST Risk Management Framework [8] and COBIT [22], among others, provide a guide for the application of risk management and good practices to ensure security and help combat cyberattacks.

Framework or standard practices	Description
ISO / IEC 27001 [19]	International standard that gathers the best practices to implement an information security management system.
NIST CSF [8]	Framework established to guide the development of cyber resilience infrastructure and help maintain a safe and secure environment.
COBIT [22]	Integrates best aspects of a company to its security, governance and IT management.
OWASP [23]	Organization promoting good practices in web-oriented development.
C2M2 [24]	Provides a detailed analysis of cybersecurity vulnerabilities identified in a critical organization.
ISO 22301 [20]	International business continuity management standard aimed at managing the global risks of each organization and its resilience capacity.
ISO 31000 [25]	ISO standard dedicated to risk management.
ENISA [21]	Major player in the cybersecurity industry works together with its stakeholders to strengthen trust in the connected economy, boost infrastructure resilience, maintain digital security for European society and citizens.

Table I
Summary of standards and best practices

IV. Towards a New Cyber-Resilience Framework

Although the NIST framework [8] can be applied to any type of organization, it requires a great implementation effort. In addition, this framework comprises 96 standards grouped into categories and subcategories. This overwhelming documentation is understandable if we consider that the NIST framework was delivered as a guide for the development of a nation's cyber-resilience infrastructure [8]. Likewise, existing cyber-resilience mechanisms in corporations, in the context of the integration of the digital supply chain, require the effective adoption of relevant existing standards, processes, and resources to achieve a good level of resilience [26].

Cyber-resilience is directly related to cybersecurity, as shown in Table II. In this regard, we propose the use of models and techniques based on machine learning that enable us to predict known and unknown attacks and to recover the system to a well-defined state (i.e., not compromised) to protect a system in a timely manner.

Appearance	Cybersecurity	Cyber-resilience
Objective	Protect information and communication technology systems.	Guarantee business continuity, under the context of preventing, detecting, containing and recovering, minimizing the exposure time and the impact on the business.
Purpose	Fail safely.	Capacity of an organization to adapt and continue with its processes and functions in adverse situations.
Orientation	Designed to apply security from outside the organization.	Build security from within the organization.
Architecture	Single-layer protection.	Multi-layer protection.
Scope	Grounded is a reactive defense.	Its principles are proactive and holistic.
Information and Communication Technologies	Integrate best IT security practices.	Integrate good practices related to IT security, business continuity, and other disciplines.

Table II
Relationships of cybersecurity and cyber-resilience.

These prediction mechanisms allow the system to put more preventive mechanisms in place, making predictions about the likelihood of attacks. A posterior diagnosis phase can help to obtain the certainty about the exploitation of vulnerabilities, and hence act in consequence. In brief, this framework should help decision-makers establish priorities and actions to mitigate the most critical vulnerabilities.

To achieve this, we need first to build a machine-learning model able to record information and to obtain the characteristics of the attack. This model needs to be trained and then tested to evaluate its efficiency, determining its precision and recall so that future attacks can be accurately predicted in advance. In addition, the classification of attacks, their categorization by similarity, the detection of attack patterns, and the detection of anomalies will allow organizations to learn from previous attacks, so as to improve their business continuity. For the construction of a prediction model for recovering, we will explore supervised, semi-supervised, and unsupervised models to find the most suitable model for our purposes.

The use of machine learning algorithms in cybersecurity has become a common practice in recent years [27]. This trend is driven by the need of detecting increasingly subtle patterns over time, with large volumes of data. Furthermore, the development and applications of machine learning methods in traditional engineering fields have also increased in recent years, and more specifically in the field of systems engineering [28]. For instance, in [29] the authors proposed a machine-learning system to detect denial of service and identity theft attacks in autonomous robots.

V. Future Directions

We envision the need of a new cyber-resilience framework as an alternative to support organizations for business continuity, which relies on machine learning techniques to anticipate the likelihood of suffering attacks.

Our road-map for developing this framework is composed of seven stages: first, the development of cyber-resilience models, especially tailored for web-oriented products; second, the identification of good practices in the management and implementation of web-oriented cyber-resilience systems; third, the design of a cyber-resilience modeling that will be the basis for carrying out the analysis and assessment of the security of the web products; fourth, the cyber-resilience analysis conducted using machine learning to mitigate risks; fifth, cyber-resilience counseling to ensure continuity of information security; sixth, a perspective on people's behavior patterns, on a cyber-resilient culture, and awareness of cybersecurity as strategies for business continuity; and last, but not least, the design of a machine-learning algorithm to identify cyberthreats in web products, which it will be later validated through test and case studies.

References

[1] Y. Cheng, Q. Wu, W. Chen, and B. Wang, "Distributed shielded execution for transmissible cyber threats analysis," *Journal of Parallel and Distributed Computing*, vol. 122, pp. 70–80, 2018.

[2] K. de Bruijn, J. Buurman, M. Mens, R. Dahm, and F. Klijn, "Resilience in practice: Five principles to enable societies to cope with extreme weather events," *Environmental Science & Policy*, vol. 70, pp. 21–30, 2017.

[3] S. Lee, S. Lee, T. Kang, M. Kwon, N. Lee, and H. Kim, "Resiliency of mobile OS security for secure personal ubiquitous computing," *Personal and Ubiquitous Computing*, vol. 22, no. 1, pp. 23–34, 2018.

[4] Y. I. Khan, E. Al-shaer, and U. Rauf, "Cyber Resilience-by-Construction: Modeling, Measuring & Verifying," in *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense*, ser. SafeConfig '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 9–14.

[5] D. Rehak, J. Markuci, M. Hromada, and K. Barcova, "Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system," *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 3–17, 2016.

[6] J. Carlson, R. Haffenden, G. Bassett, W. Buehring, M. J. Collins, S. Folga, F. Petit, J. Phillips, D. Verner, and R. Whitfield, "Resilience: Theory and Application," Argonne National Laboratory, techreport ANL/DIS-12-1, 2012.

[7] E. Viganò, M. Loi, and E. Yaghmaei, *Cybersecurity of Critical Infrastructure*. Cham: Springer International Publishing, 2020, pp. 157–177.

[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Tech. Rep., 2018.

[9] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, 1st ed. Springer International Publishing, 2017.

[10] H. Tran, E. Campos-Nanez, P. Fomin, and J. Wasek, "Cyber resilience recovery model to combat zero-day malware attacks," *Computers & Security*, vol. 61, pp. 19–31, 2016.

[11] L. Y. C. Chang, *Cybercrime and Cyber Security in ASEAN*. Cham: Springer International Publishing, 2017, pp. 135–148.

[12] Federal Bureau of Investigation, "2017 Internet Crime Report," FBI's Internet Crime Complaint Center, Tech. Rep., May 2018.

[13] J. Ferland, "Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case," *Computer Law & Security Review*, vol. 35, no. 4, pp. 369–376, 2019.

[14] F. Malecki, "Overcoming the security risks of remote working," *Computer Fraud & Security*, vol. 2020, no. 7, pp. 10–12, 2020.

[15] McAfee Labs, "McAfee Labs Threats Report," [Online; https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf], Nov. 2020, accessed on February 13, 2021.

[16] L. Y. Chang and N. Coppel, "Building cyber security awareness in a developing country: Lessons from Myanmar," *Computers & Security*, vol. 97, p. 101959, 2020.

[17] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Computers & Industrial Engineering*, vol. 149, p. 106829, 2020.

[18] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis," *Future Generation Computer Systems*, vol. 105, pp. 410–431, 2020.

[19] International Organization for Standardization, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," [Online; https://www.iso.org/standard/54534.html], Oct. 2013, accessed on February 10, 2021.

[20] ——, "ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements," [Online; https://www.iso.org/standard/75106.html], Oct. 2019, accessed on February 10, 2021.

[21] European Comission, "European Union Agency for Cybersecurity (ENISA)," [Online; https://www.enisa.europa.eu/], 2005, accessed on February 10, 2021.

[22] D. Oliver and J. Lainhart, "COBIT 5: Adding Value Through Effective Geit," *EDPACS*, vol. 46, no. 3, pp. 1–12, 2012.

[23] OWASP Foundation, "Open Web Application Security Project (OWASP)," [Online; https://owasp.org/], 2001, accessed on February 10, 2021.

[24] P. Curtis, N. Mehravari, and J. Stevens, "Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0," Carnegie Mellon University, techreport AD1026943, Apr. 2015.

[25] International Organization for Standardization, "ISO 31000:2018 Risk management — Guidelines," [Online; https://www.iso.org/standard/65694.html], Feb. 2018, accessed on February 10, 2021.

[26] M. J. Lees, M. Crawford, and C. Jansen, "Towards Industrial Cybersecurity Resilience of Multinational Corporations," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 756–761, 2018.

[27] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, "Machine Learning Security: Threats, Countermeasures, and Evaluations," *IEEE Access*, vol. 8, pp. 74 720–74 742, 2020.

[28] S. Chen, Z. Wu, and P. D. Christofides, "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control," *Computers & Chemical Engineering*, vol. 136, p. 106806, 2020.

[29] Ángel Manuel Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of Cyber-attacks to indoor real time localization systems for autonomous robots," *Robotics and Autonomous Systems*, vol. 99, pp. 75–83, 2018.