UNIVERSIDAD DE MURCIA

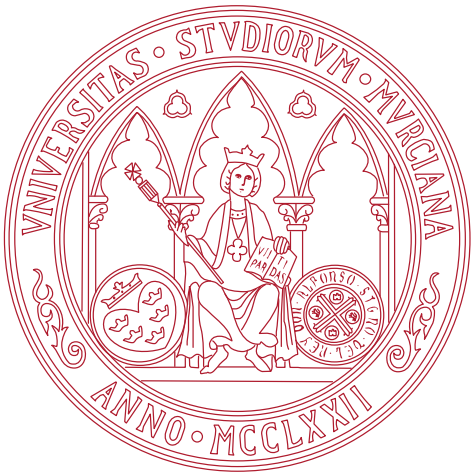
ESCUELA INTERNACIONAL DE DOCTORADO

Dynamic reaction framework against cyber attacks

Framework de reacción dinámico frente a ciber ataques

D. Pantaleone Nespoli

2021



UNIVERSITY OF MURCIA

FACULTY OF COMPUTER SCIENCE

Dynamic reaction framework against cyberattacks

Author

Pantaleone Nespoli

Thesis supervisor

Dr. **Félix Gómez Mármol**, *Ph.D.*

Murcia, 2021

The following PhD Thesis is a compilation of the next published articles, being the PhD student the main author in all of them:

- Pantaleone Nespoli, Dimitrios Papamartzivanos, Félix Gómez Mármol, Georgios Kambourakis, "**Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks**.", *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 1361–1396, 2018.
  DOI: 10.1109/COMST.2017.2781126
  JIF 2018: 22.973 (Q1)

- Pantaleone Nespoli, Félix Gómez Mármol, Jorge Maestre Vidal, "**Battling against cyberattacks: Towards pre-standardization of countermeasures**.", *Cluster Computing*, vol. 24, pp. 57–81, 2021.
  DOI: 10.1007/s10586-020-03198-9
  JIF 2019: 3.458 (Q1)

- Pantaleone Nespoli, Félix Gómez Mármol, Jorge Maestre Vidal, "**A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection**.", *IEEE Access*, vol. 9, pp. 60971–60996, 2021.
  DOI: 10.1109/ACCESS.2021.3074021
  JIF 2019: 3.745 (Q1)

Contents

Publications composing the PhD Thesis

Acknowledgements

Sono passati 4 anni. Sembra ieri quando arrivai in una città che non conoscevo, in cui le persone comunicavano in una lingua che non parlavo. Ho dovuto imparare ad adattarmi ad un contesto nuovo, ad affrontare difficoltà mai vissute prima. Ho dovuto fare tanti, tanti sacrifici, con un solo obiettivo nella mente: essere dottore di ricerca in cybersecurity.

Ed eccomi qui, 4 anni dopo, terminando la tanto desiderata tesi. Sono cambiate talmente tante cose che quasi faccio fatica a ricordare cosa c'era prima e cosa c'è adesso. Senza dubbio, posso affermare che sono cambiato io, sento di essere cresciuto umanamente e professionalmente, e ciò mi rende molto felice.

Inutile negarlo, non sarei mai riuscito a tagliare questo traguardo da solo, nonostante la caparbietà che mi contraddistingue. Mi sento fortunato perché, durante questo cammino tortuoso lungo 4 anni, sono stato accompagnato da persone meravigliose che hanno creduto in me e reso i miei giorni migliori.

Ringrazio mia madre, la donna della mia vita, che insieme a mio padre mi hanno permesso di svolgere questo percorso, sacrificandosi senza mai recriminare niente.

Ringrazio mia sorella, per avermi accompagnato con il suo amore incondizionato, e che con mio cognato mi hanno donato i regali più belli che una persona possa desiderare: i miei nipoti, a cui prometto di essere costantemente la migliore versione possibile di me.

Ringrazio la mia famiglia, che mi ha sempre sostenuto in questo lungo viaggio lontano da casa. Anche quelli che adesso sono lassù mi proteggono ed indicano la strada continuamente.

Ringrazio i miei amici in Italia, che hanno saputo accorciare le distanze in momenti difficili, e che mi fanno sentire ogni volta come se il tempo non fosse mai passato. Grazie Alfonso, Angelo, Alessio, Dario, Davide, Valentino, siete una presenza costante nella mia vita, prima, durante e dopo questa esperienza.

Ringrazio le mie amiche in Italia, il vostro affetto non ha mai conosciuto i limiti della distanza. Grazie Ada e Valentina, so di poter contare su di voi sempre e comunque.

Ringrazio la mia amica e collega Valentina, sei entrata a far parte della mia vita personale e professionale nel momento più difficile per tutti, sei la dimostrazione che le cose belle possono accadere anche nei periodi più oscuri.

Doy las gracias a Bea, mi amor, que me ha acompañado y ayudado todos los días, has creído en mi desde el primer instante. Contigo he encontrado la familia que no tenía aquí en Murcia.

Doy las gracias a los muchísimos erasmus que han pasado su tiempo en Murcia conmigo. Vuestra amistad ha hecho el camino más ameno. Entre todos, un puesto especial en mi

corazón lo tienen Alexandra, Paola, Sara y Barbara, amigas verdaderas, que espero tener conmigo por el resto de mi vida.

Doy las gracias a mis amigos de Murcia, mi familia en España, que me han acogido y ayudado como si fuera uno de ellos desde el principio. Sois muchos, la verdad, y también por esto me siento afortunado. Así que, muchas gracias Fran, Alberto, Javi, Raba, LuisMi, Tito, Rubén, Juanjo, Fernando, Alejandro, Carla, Clara, Helena y Luisa, sin vosotros los días no serían iguales.

Doy las gracias a mi grupo de investigación, todos y cada uno de mis compañeros de trabajo me han ayudado en lo personal y en lo profesional de igual manera. Así que muchas gracias Mattia, Sergio, Javier, Manuel, Lorenzo, Gregorio y todos los demás del Lab, os debo mucho.

Doy las gracias a Daniel, amigo y colaborador en Bogotá, el trabajo juntos ha sido una experiencia fantástica, y espero poder seguir así por mucho tiempo.

Doy la gracias a Jorge, supervisor y compañero de INDRA, con tu apoyo mi trayectoria de investigación ha tomado una perspectiva algo distinta y muy potente.

Thanks Dimitris and Georgios, Greek colleagues, you helped me develop into the researcher I am today.

Por último, y sin duda la persona a la cual más debo, quiero agradecer a mi supervisor Félix. Si estoy en Murcia, si estoy a punto de terminar este camino, es porque tú has luchado a mi lado sin parar nunca. Me has enseñado todo lo que sé del mundo de la investigación, me has ayudado en los momentos más obscuros durante estos 4 años, has sido al mismo tiempo un mentor, un amigo, un hermano mayor. Espero un día poder devolverte todo lo que me has dado con generosidad.

Grazie a tutti, spero di continuare ad avervi nella mia vita, mi rendete una persona migliore.

Abstract

I Introduction and motivation

Undoubtedly, the importance of Information and Communication Technology (ICT) systems is reaching previously-unseen peaks. That is, modern network infrastructures are constantly expanding in size and value to provide services to humans as an ultimate goal. The consequences of such an expansion are directly reflected in our everyday life: billions of people are willing to consume those generated services to improve their overall quality of life, both from a personal and professional perspective. Such demand requires to be served by a plethora of devices, which are growing in quantity and ubiquity. Specifically, up-to-date studies report that the number of devices connected to the Internet is expected to be 20 billion, exceeding the number of people connected to such network by three to five times [1]. Therefore, it should not be a surprise that individuals are more and more dependent on technology. Additionally, the fresh advance of fifth-generation (5G) and beyond 5G (B5G) platforms further pushes such a digital revolution. In fact, thanks to those platforms, the connectivity is able to reach an astonishing speed with incredibly low latency. On top of that, the rise of disruptive technologies (e.g., Blockchain [2]) and paradigms (e.g., Internet of Things (IoT) [3]) has paved the path to significant contributions from both the industrial and research worlds.

Nevertheless, the digital revolution does not come without a price. Indeed, the security of the provided products or services is frequently neglected since the Time To Market (TTM) is becoming extremely short due to the higher demand [4]. Triggered by the potential high profit of cybercrime, the number of ill-motivated actors has significantly increased during recent years. Those delinquents are trying to perform malicious actions against ICT systems worldwide to disrupt the Confidentiality, Integrity, and Availability (CIA) attributes of such systems [5], consequently damaging the provided services and compromising the related information. Also, by leveraging millions of devices from around the globe, attackers are able to recruit an army of machines to launch world-record Distributed Denial of Service (DDoS) offensives, devastating state-of-the-art datacenters [6]. Yet, the motivations of those attackers changed over the years. Specifically, as the ICT systems were rising, attackers were skilled individuals who were performing their malicious actions just to prove their capacities. Nowadays, they can be depicted as militarized groups of ill-motivated persons that often sell their duties to the best bidding [7]. To this extent, many of the launched attacks today are incredibly disruptive, involving nations' defensive agencies in this endless battle [8]. That is, the concept of cyber warfare has recently be-

come a crucial affair to deal with for the nations since the battlefield also includes the cyberspace [9].

In such an alarming context, one could quickly notice that cybersecurity and cyber defense play a vital role in shielding hyper-connected devices and protecting the cyberspace. Nonetheless, battling against offensive incidents represents a particularly complicated task because of the inherently dynamic nature of ICT systems and the diversity of potential attack vectors. Specifically, medium-to-high critical vulnerabilities are reported on a daily basis, affecting a myriad of different systems' assets [10]. Besides, the size of the previously mentioned infrastructures generates hardly manageable dependencies among the assets and services, which attackers can leverage to execute multi-step attacks up to their final goal [11]. In the context of this PhD Thesis, the overall cybersecurity responsibility has been broken into four main tasks, which are strongly connected as each of them gives input to the next one, building a protective cycle:

- **Prevention**: the prevention phase is responsible for continuously monitoring the underlying system to discover any security flaw (e.g., vulnerabilities, misconfigurations) and enforce security measures to solve it.

- **Detection**: assuming that the monitored system is (or will be) vulnerable to potential threats, the detection phase is in charge of accurately identifying and promptly reporting intrusive incidents that entail the exploitation of security flaws.

- **Reaction**: when an incident has been reported, the reaction has to be fired to mitigate or even eradicate the harmful attack, evaluating as well the impact of the incident and the consequences of the counteractions. In particular, this PhD Thesis will focus on this specific phase.

- **Forensics**: once the incident has been wiped out from the system, the forensic step needs to analyze the actions recorded during the previous phases. Such an operation allows one to discover what went wrong and avoid similar episodes in the future.

Among those phases, the reaction can be described as a fundamental step in the endless arms race between offensive and defensive formations. Typically, the reaction is tasked with a dual objective: on the one hand, the optimal set of countermeasures has to be selected to block the ongoing threat immediately [12]. On the other hand, it must indicate the collection of actions to heal the system and bring it back to a normal operational state [13]. Surprisingly, the reaction stage has received considerably less attention from both the academy and industry than the detection. The main reasons for this discrepancy could be assigned to the several challenges corroborating the reaction ecosystem, which are profoundly discussed and tackled within this PhD Thesis. To this extent, it is worth remarking on the crucial function executed by the security administrators of the system. Concretely, they are responsible for cherry-picking the most appropriate actions at each step of the above-mentioned cybersecurity phases. Regarding the reaction step, the security administrators bear the burden of balancing the inherent tradeoff between the effectiveness of the response and its potential negative impact on the system assets, always working with strict budget constraints [14]. In a digital world moving toward the complete automation of the processes (included security ones), we contemplate the role of the security administrators as central in each reaction strategy, being those who make the decisions leveraging their cybersecurity background.

Furthermore, throughout this PhD Thesis, another essential concept is the difference between the two primary reaction approaches, namely, static and dynamic:

- **Static reaction**: this response is responsible for proactively working against possible security incidents. Mainly, it deals with identifying the system characteristics with a particular focus on weaknesses, vulnerabilities, and exposures. Such a task leads to a correct risk estimation, but it is usually not trivial due to the complexity and size of the system.
- **Dynamic reaction**: this approach is in charge of counteracting potential ongoing attacks. In this case, apart from a holistic knowledge of the system, the evaluation of the attacker's objectives and response time are fundamental, among others.

In this regard, it is clear that the dynamic reaction requires more computational power, and the countermeasures selections should be made balancing the cost-benefit tradeoff in near real-time. Thus, the scalability of the proposed dynamic solutions in the literature tends to be inadequate, reflected in the authors' tiny testing environments. Moreover, the reaction works do not adopt a standard assessment methodology to provide a quantitative analysis of the defense strategy they propose. One could say that a standard model which can assess the tradeoff between attack impact and defense cost in enforcing countermeasures is necessary for every reaction framework. Furthermore, the battle against cyberattacks should rely on comprehensive and commonly agreed countermeasures knowledge. Indeed, the reaction methodologies presented in the literature propose to apply ad-hoc remediations, which are often based on authors' subjective beliefs.

II Objectives

The main objective of this PhD Thesis is to study, analyze and address the principal limitations of the state-of-the-art reaction frameworks, leading to the development of a scalable and robust countermeasures selection system, which can compute the optimal reaction starting from an Intrusion Detection System (IDS) alert or any security flaw discovery procedure. Furthermore, such a reaction should rely on a common and shared countermeasure representation that leverages comprehensive countermeasures knowledge.

More specifically, the main goal may be divided into several sub-objectives, which are listed as follows:

1. Analyze the current state-of-the-art proposals regarding the reaction ecosystem.
2. Identify major advantages and potential drawbacks of the studied reaction frameworks.
3. Highlight the current challenges of the field and write future research directions.
4. Propose a standard representation of the countermeasure objects.
5. Study the feasibility of the standard countermeasures proposal in different real-case scenarios.
6. Introduce an index to assess the benefit of the enforcement of a single or multiple countermeasures on the same asset, considering the effectiveness, negative impact, and cost.
7. Present a novel and robust reaction methodology to select the optimal set of countermeasures.
8. Estimate the performance of the suggested methodology throughout exhaustive experiments.

III Methodology

Since this PhD Thesis was conceived from its very beginning as a publications compendium, all the work carried out throughout the doctorate path was directed towards this goal. It is worth noticing that the PhD Thesis is co-supervised and co-funded by Indra[1], an international enterprise that integrated some of the research outcomes of this work into their portfolio of products and solutions for cyber defense. Consequently, the PhD Thesis objectives described in the previous section have been agreed upon between the University of Murcia and Indra to ensure complete alignment between the scientific goals and the company's needs.

Indra is a leading provider of solutions for the defense sector, which has identified the dynamic reaction against cyber threats as a baseline for strengthening its Cyber Situation Awareness products. Specifically, the reaction phase entails a strategic area in its core business activities for the defense market, where essential resources are already being invested in order to develop a new portfolio of cyber defense products around cyber situational awareness-related capabilities. Some of the targeted stakeholders to leverage the PhD Thesis' results are the National Ministers of Defence (MoDs), the European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), or the North Atlantic Treaty Organization (NATO). In this regard, this PhD Thesis entails an added-value contribution that Indra expects to exploit commercially soon after the PhD Thesis outcomes have gone into production.

III.1 Survey of reaction frameworks

The first milestone of this PhD Thesis has to do with the study of state-of-the-art reaction frameworks, referred to in its first chapter (A Comprehensive Survey on Reaction Frameworks (Article 1–IEEECOMST)). Collecting, studying, and analyzing the major pertinent works in the reactions ecosystem represents a crucial step. Indeed, it allows one to highlight the field's challenges and draw future directions for the researchers. More specifically, the survey includes the 24 most remarkable works dealing with reaction against cyberattacks over a period of 5 years (i.e., from 2012 to 2016). The study has a dual goal: first, it aims to deeply analyze the significant proposals in the field. Second, it offers a comprehensive discussion and a side-by-side comparison among the selected works based on seven common criteria. In particular, the identified criteria are:

- **Attack modeling**: a formal model to describe potential attackers' actions focusing on the security flaws present within the protected system.
- **Countermeasure provision technique**: the methodology (and related metrics) to select and enforce a set of countermeasures on the system's assets.
- **Outcomes assessment**: the evaluation of the outcome of the analyzed works, i.e., the provisioning of remediation actions. In particular, two characteristics are extracted, namely, testbed and admin's role.
- **Type of reaction**: the reaction is envisioned following two main approaches, namely, static and dynamic reaction, as mentioned before.
- **Use of standards**: the use of standards in the design, development, and assessment of the reaction strategies facilitates the comparison among the published works and solutions, giving a quantitative and qualitative measurement of their effectiveness.

[1] https://www.indracompany.com

- **Automation level**: due to the potential complexity of the reaction framework, the level of automation is considered an essential factor.
- **Performance**: factors that strongly impact the implementation of the countermeasure strategy are collected and detailed.

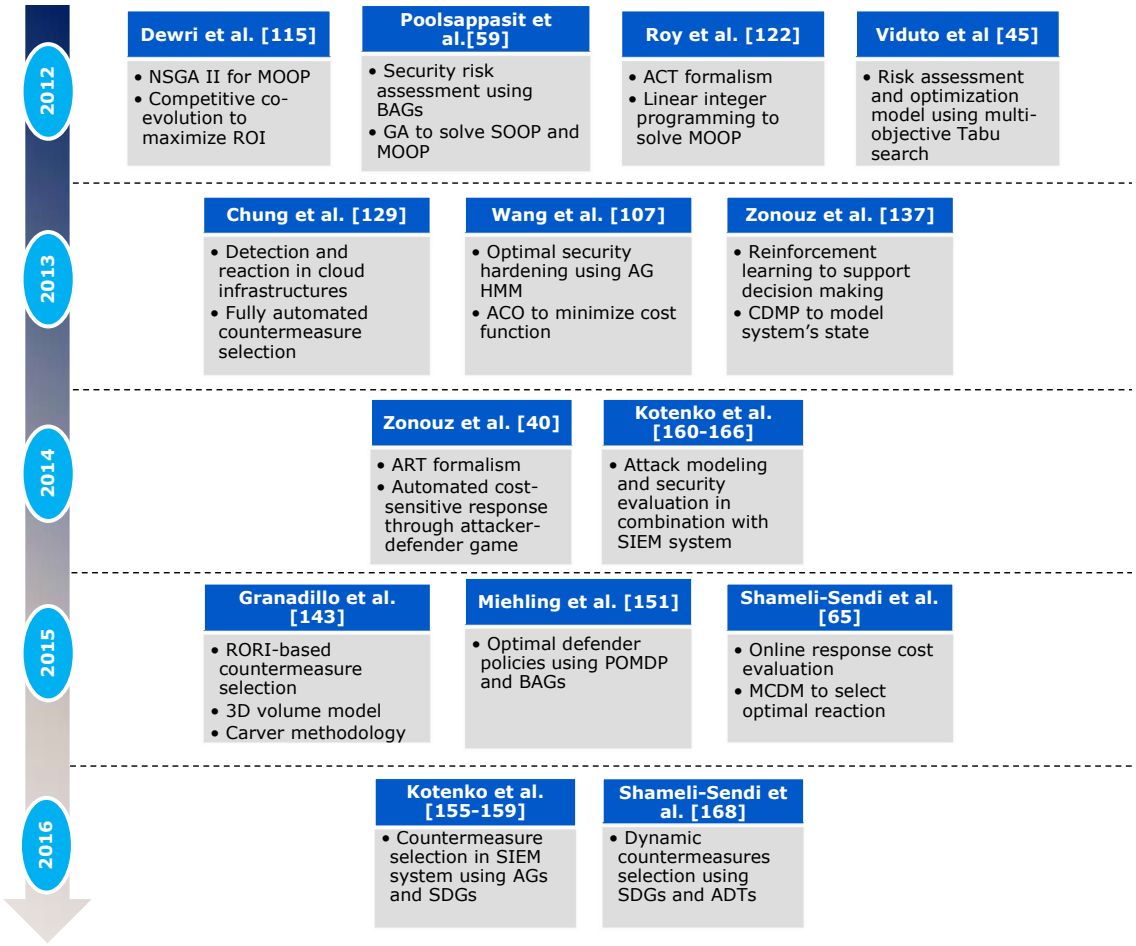


Figure 1: Timeline of the surveyed works, highlighting on their novelty and core characteristics.

A graphical summary of the surveyed works with reference to the publication year and their main features is shown in Figure 1. Particularly, such a figure reviews the evolution of the analyzed research topic, where authors provide different reaction proposals against cyberattacks. Then, both positive and negative aspects of each work are highlighted.

Based on the in-depth analysis conducted, six research challenges were identified that seem to be the most prominent in the development of a reaction solution:

- **Scalability**: one of the main drawbacks of the surveyed works is the poor scalability. Specifically, attack modeling is recognized as the leading cause of such a deficiency.
- **Countermeasure knowledge**: each of the studied proposals utilized only a reduced set of countermeasures enforced over the assets against specific attacks.
- **Standard representation**: another lack arisen during the study consists in the absence of a standard representation of countermeasure.

- **Countermeasures-attacks correlation**: Once a full-fledged set of countermeasures has been built, careful analysis of the correlation between remediations and attacks also represents a primary need.
- **Metrics and scoring systems**: a noticeable lack of specific and commonly-used measurement system to quantitatively analyze the reaction proposals has been found among the analyzed works.
- **Mitigating zero-day attacks**: the vast majority of the presented countermeasure strategies neglect the reaction against unknown offensive incidents.

For each of them, a number of solutions have been proposed to potentially contribute to this timely research area.

III.2 Standard countermeasure proposal

Starting from the challenges highlighted in the previous survey, another significant achievement of this PhD Thesis is the proposal of a standard representation of a countermeasure, detailing with fine granularity the fields that are necessary to encompass the remediation object. As detailed in the second chapter (Towards Pre-standardization of Countermeasures (Article 2–`Clus`)), such a representation serves as a starting point towards the standardization of the countermeasures within the reaction ecosystem, enabling continuous reaction knowledge sharing among security teams worldwide. Additionally, a standard representation of remediation objects serves as a basis to build robust reaction strategies, constantly refreshed with new instances.

The proposed representation considers specific characteristics of each countermeasure (e.g., effectiveness, impact, cost, possible parameters), but it also leverages the security knowledge that is already present within other widely employed security repositories (e.g., platforms, attacks, vulnerabilities, configurations knowledge bases). To this extent, the reuse of already mature and shared security know-how represents a significant pointer to adopt a standard format also for the countermeasures ultimately.

$$cm_{ID} = (\underbrace{ID, Eff, Imp, Cost, \Omega_c, \Omega_p, \Omega_v, \Omega_a, \phi}_{mandatory}, \underbrace{P, \delta}_{optional}) \tag{1}$$

More specifically, the proposed definition is depicted in Equation 1, while its elements are detailed in the following:

- $ID \in \mathbb{N}$ is the unique identifier of the countermeasure.
- $Eff \in \{L, M, H, X\}$ represents the residual effectiveness of the countermeasure, referring to its capability to block the threat.
- $Imp \in \{L, M, H, X\}$ refers to the residual impact of the countermeasure since it can negatively impact the corresponding asset(s) within the monitored system.
- $Cost \in \mathbb{R}^+$ represents the residual cost of the countermeasure, which contemplates deployment, maintenance, and indirect costs.
- $\Omega_c = \{c_i \in C\}$ is the link to common configuration knowledge base C to which the designed asset refers.
- $\Omega_p = \{p_i \in P\}$ is the link to common platform knowledge base P to which the designed asset refers.

- $\Omega_v = \{v_i \in V\}$ is the link to common vulnerability knowledge base V to which the exploited vulnerability refers.
- $\Omega_a = \{a_i \in A\}$ is the link to common attack knowledge base A which the countermeasure counteracts.
- ϕ describes the enforcement of the countermeasure in a machine-readable format.
- $P = \{p_1, p_2, ..., p_n\}$, with $n \geq 0$, describes the parameter(s) a certain countermeasure may need in order to be implemented.
- δ includes additional information about the countermeasure, particularly:
  - a textual description, in human-understandable language.
  - a field indicating whether the deployment of the countermeasure demands software or hardware changes.
  - a flag specifying if the countermeasure is static or dynamic.
  - a field expressing whether the countermeasure is of short-term or long-term duration within the reaction strategy.
  - examples of the enforcement (e.g., in pseudocode).
  - if applied for cyber defense, linkage to military tactical, strategic, or operational decisions.

In the context of this research, a set of discrete values is used to assess the residual effectiveness and impact of the countermeasures, namely, L (Low), M (Medium), H (High), and X (Not Defined). Specifically, the proposed representation leverages both mandatory and optional fields. The former are considered to be rigorously needed to correctly encompass the essential features of a countermeasure, while the latter are presented to further characterize such remediation, not being crucial for its representation or implementation. However, each of the suggested fields is described with adequate detail, discussing the main reason for its choice within the representation.

Moreover, to prove the applicability of the approach, examples of countermeasures enforcement in real scenarios are presented. Notably, a smart home scenario, an enterprise network scenario, and an industrial infrastructure scenario are introduced. By leveraging the proposed representation, the countermeasure objects are correctly corroborated and enforced, being effective against active threats and protecting the system's assets.

Finally, an in-depth discussion on the proposed standard representation is elaborated, debating the key features and potential improvements towards a full-fledged countermeasure strategy.

III.3 AIS-powered reaction

In turn, another notable achievement of this PhD Thesis consists in the design and implementation of a novel and scalable methodology to compute the optimal set of countermeasures against cyber intrusions, as reported in the third chapter of this document (AIS-powered Optimal Countermeasures Selection (Article 3–`IEEEAccess`)). Such a solution leverages the outstanding capabilities of an Artificial Immune System (AIS). This bio-inspired technique is able to compute optimal outcomes in a more than acceptable time thanks to the continuous cloning and mutation phases. Besides, the countermeasures are encapsulated in the proposed standard representation, strengthening the interoperability of the reaction strategies.

Specifically, a preliminary modeling phase is performed to translate the immuno-related concepts of the AIS to the cybersecurity reaction context. To this extent, the assets $A_x \in A$ are the main focus of the reaction process. At any moment, those assets demand protection against potential threats $\tau_k \in T$, i.e., vulnerabilities and attacks, by minimizing the risk to which they are exposed. In this direction, the threats T represent the *antigens* against which the AIS-powered reaction calculates the optimal response using *antibodies*, i.e., the set of countermeasures CM.

To compute the atomic countermeasures $cm_i \in CM$ that belong to the optimal solution, the countermeasure benefit $B(cm_i)$ is proposed. Such an index contemplates the advantages of enforcing specific reaction steps over a certain asset by balancing the tradeoff between their effectiveness and their negative impact and cost. The dissertation is then enriched to consider the possibility of implementing a set of countermeasures on a particular asset simultaneously.

After a profound modeling phase, the AIS-powered reaction is described to minimize the difference between the risk to which the assets are exposed (i.e., the measured risk $RL(\tau_k, A_x)$) and the acceptable risk level assigned to each asset $\widetilde{RL}(A_x)$ by applying a set of countermeasures $CM_j(A_x)$. Concretely, the AIS-powered reaction is capable of determining the optimal set of atomic countermeasures by continuously cloning and mutating the antibodies within the solution space.

Figure 2 illustrates an example of the steps of the AIS-powered reaction. First, an initial set of antibodies (i.e., set of atomic countermeasures) is randomly generated. In the proposed example, $\mathbb{CM} = \{CM_1, CM_2, CM_3\}$. Then, the affinity of the generated antibodies is computed, i.e., the ability to reduce the difference between the measured and acceptable risk is measured. Assuming that the best antibody is CM_1 and the cloning factor $K = 1$, such an antibody is cloned and, successively, mutated. Supposing that the affinity of the clone CM_1' is still better than the average affinity, it is included in the solution space $\mathbb{CM}$, replacing the worst one, e.g., CM_3. Finally, the remaining worst antibody within $\mathbb{CM}$, say, CM_2, is replaced with a randomly generated one to start another iteration of the AIS reaction.

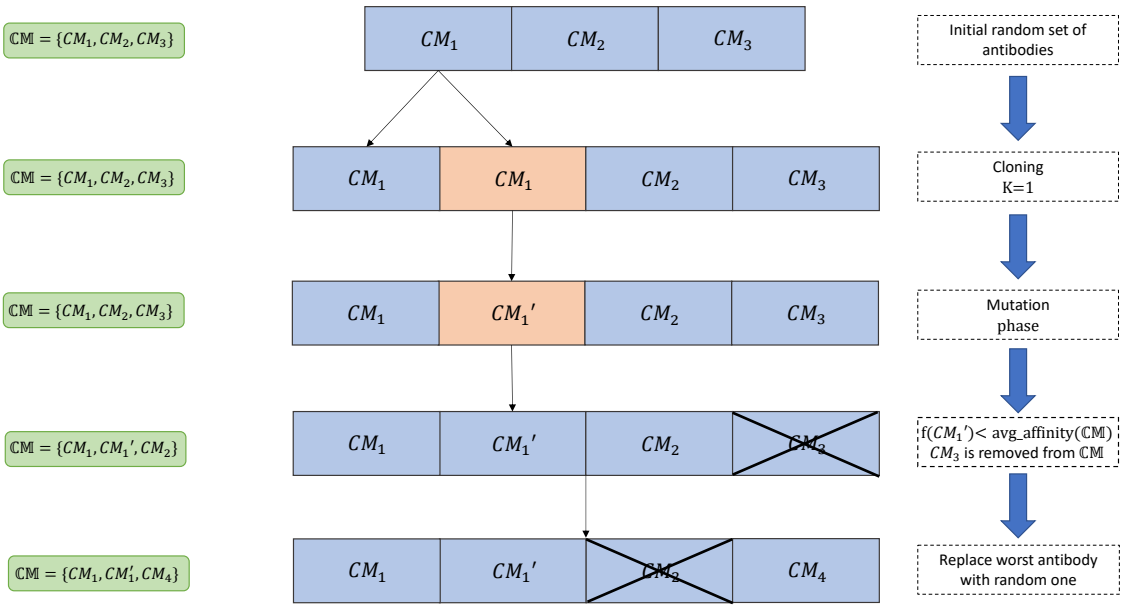


Figure 2: AIS-powered reaction steps.

Then, static and dynamic versions of the AIS-powered reactions are presented, depending on the phase in which the procedure is fired. Additionally, a context-aware stop condition is suggested which, based on the witnessed initial fitness, assigns specific values to the input parameters of the procedure to calculate solutions promptly when the initial fitness is high (i.e., the assets are exposed to a high-risk situation), while it computes longer searching for better solutions when the initial fitness is low.

Furthermore, the proposed methodology is stressed through an intensive experimental session, in which the parameters of the underlying scenarios (i.e., threats, assets, and countermeasures) were randomly generated to better argue on the capabilities of the methodology by introducing randomness. In this direction, the experiments demonstrate the capabilities and robustness of the procedure, helping human actors in the decision-making procedure.

IV Other relevant publications

Besides, during his PhD Thesis, the doctoral student also participated in several research projects related to cybersecurity aspects, leading to the relevant publications that enriched his skills both from a research and team-working perspective. In the following, the publications are grouped based on the research project or collaboration to which they are connected.

IV.1 A SIEM solution deployment for the protection of information assets

In this project, the security conditions of IoT devices are revised to propose a cybersecurity architecture for IoT systems entailing a holistic security paradigm for the protection of information assets. Such a solution should be easy to follow by technology developers, IT areas, and users, strengthening this way the technological environments of organizations, as well as the individuals using them.

This project has been carried out along with the Colombian Engineering School "Julio Garavito", Bogotá, Colombia, resulting in an interesting international collaboration and a very fruitful visit to Bogotá. In the following, the published articles are listed, stating in the case of journal publications their Journal Impact Factor (JIF), as well as the quartile they belong to (Q1, Q2, Q3, or Q4):

- Daniel O. Díaz López, María Blanco Uribe, Claudia Santiago Cely, Andrés Vega Torres, Nicolás Moreno Guataquira, Stefany Moron Castro, Pantaleone Nespoli, Félix Gómez Mármol, "**Shielding IoT against cyber-attacks: An event-based approach using SIEM**.", *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–18, 2018.
  DOI: 10.1155/2018/3029638
  JIF 2018: 1.396 (Q3)

- Daniel O. Díaz López, Maria Blanco Uribe, Claudia P. Santiago Cely, Daniel F. Tarquino Murgueitio, Edwin S. García García, Pantaleone Nespoli, Félix Gómez Mármol, "**Developing secure IoT services? A security-oriented review of IoT platforms**.", *Symmetry*, vol. 10, pp. 1–34, 2018.
  DOI: 10.3390/sym10120669
  JIF 2018: 2.143 (Q2)

- Juan Velandia Botello, Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel O Díaz López, Pantaleone Nespoli, Félix Gómez Mármol, "**BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM**.", *Sensors, Special Issue on Blockchain Security and Privacy for the Internet of Things*, vol. 20, pp. 1–22, 2019.
  DOI: 10.3390/s20164636
  JIF 2019: 3.275 (Q1)

IV.2 COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things

The COSMOS project intends to develop novel and innovative solutions to provide sophisticated protection mechanisms to IoT devices. In particular, its main goal lies in the development of the so-called collaborative, seamless, and adaptive sentinels, which automatically shield the surrounding IoT devices against potential threats.

This project has been funded by a Leonardo Grant awarded by the BBVA Foundation[2] and realized at the University of Murcia in collaboration with several other research centers [3]. The related publications are listed as follows:

- Pantaleone Nespoli, Félix Gómez Mármol, "**e-Health Wireless IDS with SIEM integration**.", *IEEE Wireless Communication and Networking Conference (WCNC 2018), Barcelona, Spain.*

- David E. Useche Peláez, Daniel O. Díaz López, Pantaleone Nespoli, Félix Gómez Mármol, "**TRIS: a Three-Rings IoT Sentinel to protect against cyber-threats**.", *Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2018), Valencia, Spain.*

- Pantaleone Nespoli, David E. Useche Peláez, Daniel O. Díaz López, Félix Gómez Mármol, "**COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things**.", *Sensors, Special Issue on Sensor Systems for Internet of Things*, vol. 19, pp. 1–29, 2019.
  DOI: 10.3390/s19071492
  JIF 2019: 3.275 (Q1)

- Pantaleone Nespoli, Daniel O. Díaz López, Félix Gómez Mármol, "**Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices**.", *Journal of Information Security and Applications, Special Issue on Cybersecurity Trends*, vol. 60, p. 102878, 2021.
  DOI: 10.1016/j.jisa.2021.102878
  JIF 2019: 2.327 (Q3)

IV.3 AUTHCODE: AUTHentication for Continuous access On DEvices

Continuous authentication on mobile devices aims to identify the owner (or owners) of a given device at any moment. The main benefit of continuous authentication consists in improving the user experience when using services or applications on their mobile devices, avoiding complex access credentials.

[2] https://www.fbbva.es/en/
[3] https://webs.um.es/felixgm/projects/cosmos/

This project has been funded by the Seneca Foundation [4] and accomplished at the University of Murcia. In the following, the published research items are listed:

- Pantaleone Nespoli, Mattia Zago, Alberto Huertas Celdrán, Manuel Gil Pérez, Félix Gómez Mármol, Félix J. García Clemente, "**A Dynamic Continuous Authentication Framework in IoT-Enabled Environments**.", *Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2018), Valencia, Spain.*

- Pantaleone Nespoli, Mattia Zago, Alberto Huertas Celdrán, Manuel Gil Pérez, Félix Gómez Mármol, Félix J. García Clemente, "**PALOT: Profiling and Authenticating users Leveraging internet Of Things**.", *Sensors, Special Issue on Sensor Systems for Internet of Things*, vol 19, pp. 1–26, 2019.
  DOI: 10.3390/s19122832
  JIF 2019: 3.275 (Q1)

- Pedro M Sánchez Sánchez, José M Jorquera Valero, Mattia Zago, Alberto Huertas Celdrán, Lorenzo Fernández Maimó, Eduardo López Bernal, Sergio López Bernal, Javier Martínez Valverde, Pantaleone Nespoli, Javier Pastor Galindo, Ángel L Perales Gómez, Manuel Gil Pérez, Gregorio Martínez Pérez, "**BEHACOM-a dataset modelling users' behaviour in computers**.", *Data in Brief*, vol. 31, pp. 1–12, 2020.
  DOI: 10.1016/j.dib.2020.105767
  SJR 2019: 0.105 (Q4)

IV.4 BotBusters: Hunting bots in social media

The BotBusters project aims at providing Artificial Intelligence (AI) solutions to raise users' awareness from the coordinated social bots' activities. Recently, a significant rise of ill-motivated social bots has been witnessed to manipulate the social network community. Social bots nowadays constitute armies controlled by malefactors who aim to manipulate and deceive media users.

This project has been granted the Regional Winner prize at the Ericsson Innovation Award 2018[5]. It has been created as a part of a research collaboration between students from the University of Murcia (including the doctoral student) and the University of Aegean (Greece).

The related publications are listed as follows:

- Javier Pastor-Galindo, Pantaleone Nespoli, Félix Gómez Mármol, Gregorio Martínez Pérez, "**OSINT is the next Internet goldmine: Spain as an unexplored territory**.", *Fifth National Conference on Cybersecurity (JNIC 2019), Cáceres, Spain.*

- Mattia Zago, Pantaleone Nespoli, Dimitrios Papamartzivanos, Manuel Gil Pérez, Félix Gómez Mármol, Georgios Kambourakis, Gregorio Martínez Pérez, "**Screening out social bots interference: are there any silver bullet?**.", *IEEE Communications Magazine*, vol. 5, pp. 98–104, 2019.
  DOI: 10.1109/MCOM.2019.1800520
  JIF 2019: 11.052 (Q1)

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez

[4] https://www.fseneca.es/
[5] https://bit.ly/2RZhYr8

Pérez, Félix Gómez Mármol, "**Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**.", *IEEE Transactions on Network and Service Management, Special Issue on Data Analytics and Machine Learning for Network and Service Management*, vol. 20, pp. 2156–2170, 2020.
DOI: 10.1109/TNSM.2020.3031573
JIF 2019: 3.878 (Q1)

- Javier Pastor-Galindo, Pantaleone Nespoli, Félix Gómez Mármol, Gregorio Martínez Pérez, "**The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends**.", *IEEE Access*, vol. 8, pp. 10282–10304, 2020.
DOI: 10.1109/ACCESS.2020.2965257
JIF 2019: 3.745 (Q1)

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez Pérez, Félix Gómez Mármol, "**Twitter social bots: the 2019 Spanish general election data**.", *Data in Brief*, vol. 32, pp. 1–10, 2020.
DOI: 10.1016/j.dib.2020.106047
SJR 2019: 0.105 (Q4)

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez Pérez, Félix Gómez Mármol, "**A Review of Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**.", *Sixth National Conference on Cybersecurity (JNIC 2021), Castilla-La Mancha, Spain.*

IV.5 COnVIDa: COVID19 multidisciplinary data collection and dashboard

COnVIDa[6] is a web-based tool developed by the Cybersecurity and Data Science Laboratory at the University of Murcia that efficiently gathers data related to the COVID19 pandemic from different data sources in the context of Spain and visualizes them in a dashboard. To this extent, COnVIDa can be described as our small contribution to the pandemic battle.

The main research article related to this project is reported in the following:

- Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Javier Pastor Galindo, Pantaleone Nespoli, Félix J. García Clemente, Félix Gómez Mármol. "**COnVIDa: COVID19 multidisciplinary data collection and dashboard**.", *Journal of Biomedical Informatics, Special Issue on Novel Informatics Approaches to COVID-19 Research*, vol. 117, p. 103760, 2021.
DOI: 10.1016/j.jbi.2021.103760
JIF 2019: 3.526 (Q2)

IV.6 COBRA: Adaptive and customizable hyper-realistic APT simulation cyber maneuvers and cyber defense training using gamification

This project aims to develop hyper-realistic Advanced Persistent Threats (APTs) and network topologies and traffic simulation modules that simulate realistic scenarios to be

[6] https://convida.inf.um.es/

integrated into Cyber Ranges, with a module that allows the development of parameterizable and randomizable template cyber maneuver scenarios. The Cyber Range will be integrated with gamification and adaptive learning elements to make the learning process more motivating and adaptive.

This project has been found by the Spanish Ministry of Defence through Grant 10032/20/0035/00.

The related publications are listed as follows:

- Félix Gómez Mármol, José A. Ruipérez-Valiente, Pantaleone Nespoli, Gregorio Martínez Pérez,Diego Rivera Pinto, Xavier Larriva Novo, Manuel Álvarez-Campana, Víctor Villagrá González, Jorge Maestre Vidal, Francisco A. Rodriguez López, Miguel Páramo Castrillo, Javier I. Rojo Lacal, Ramón García-Abril Alonso, "**COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación**.", *Sixth National Conference on Cybersecurity (JNIC 2021), Castilla-La Mancha, Spain.*

V Conclusions and future work

The digital revolution is happening in front of our eyes, and it is changing our lives. Indeed, individuals rely more and more on the services offered by modern network infrastructures, willing to enhance their quality of life. The outstanding hyperconnectivity of the devices and the way humans can communicate among themselves were unbelievable only some years ago.

Nonetheless, the wide range of opportunities and the significant economic growth offered by such a revolution also carries along adverse outgrowths. In fact, we are also witnessing the rise of ill-motivated organizations whose main objective is to hit network infrastructures for economic and strategic purposes. No one is excluded from this endless battle: from citizens to governments, cybercriminals are threatening entities worldwide ruthlessly.

In such a dangerous scenario, security mechanisms to protect cyberspace represent a need more than ever. That is, cybersecurity and cyber defense are essential to defend ICT systems from cyber assaults. Among the four principal phases of cyber defense (prevention, detection, reaction, and forensics), the reaction against cyberattacks can be depicted as crucial to dynamically eradicate potential threats within the monitored system and, subsequently, heal related assets. Surprisingly, the reaction phase has received considerably less attention compared to the other cybersecurity ones, mainly due to the difficulties that it faces.

Aiming to contribute to the reactions ecosystem, this PhD Thesis focuses on analyzing the challenges of the field and proposing effective solutions. Bearing in mind the objectives enumerated in Section II, the following leading contributions have been achieved:

i) firstly, the in-depth study of the state-of-the-art reaction frameworks. Those response strategies have been compared side-by-side based on seven common criteria, highlighting the challenges that this field still poses, as reported in Article 1–`IEEECOMST`.

ii) secondly, the proposal of a standard countermeasure representation, aiming to boost the reactions knowledge sharing between security teams and to build robust response plans, as detailed in Article 2–`Clus`.

iii) thirdly, the design and implementation of a novel reaction framework that leverages the outstanding features of the AIS. The proposed methodology is able to cherry-pick the optimal set of atomic countermeasures to be fired against identified threats within the protected system in an effective and efficient manner, as described in Article 3–`IEEEAccess`.

Those contributions have been published in top-tier journals to disseminate the findings and possibly impact the research community as an ultimate goal. Additionally, the outcomes have been supervised and shared with Indra, aiming to exploit them in its core business activities for the defense market.

However, there is still a long way to go in the arm-race between reaction strategies and cybercriminals. Indeed, some challenges still appear unsolved and will require significant contributions in the future.

Specifically, there is an evident lack of a commonly used and shared countermeasures measurement system. So far, several indexes have been proposed in the literature, trying to capture different aspects of the remediation steps. Nevertheless, the creation of a standard countermeasure scoring system, leveraging other existing assessing frameworks, would be highly beneficial for each reaction strategy since its outcomes can be compared

with more equity. In this sense, the standard countermeasure representation proposal shall be considered a starting point toward this goal.

Additionally, the designed AIS-powered reaction methodology has been tested by simulating the underlying monitored system during the experiments. To this extent, one could say that it would be interesting to employ the proposed methodology in a real use-case scenario, studying the feasibility of applying the AIS reaction with real network traffic from the detection of the threat to the enforcement of the countermeasure. This security information flow would surely benefit from using an attack model (e.g., Attack Graph, Attack Tree, etc.) to predict attacker moves and objectives. Possibly, such a full-fledged detection-reaction framework will require the joint efforts of different research institutions, which will fit in the context of a powerful research project proposal. Also, a meta-optimization method to improve the selection of the AIS response is considered of great interest. In this direction, the doctoral student is currently working on proposing an evolutive methodology (i.e., Genetic Algorithm) to optimize those parameters and prove the robustness of the AIS-powered reaction.

Last but not least, the analysis of enriching the reaction strategies with offensive countermeasures is a subject worthy of study. Concretely, due to the highly constructive partnership with Indra, which features various military customers within its portfolio, the possibility of study, analysis, and implementation of offensive countermeasures represents an interesting future line of work. For example, this is a topic of great interest for the European Cyber Situational Awareness Platform (ECYSAP), whose development is led by Indra. In this context, the ability to provide an active response to cyber threats, which shall be proportional and acceptable in both technical and regulatory terms (doctrine, ethical framework, legislation, rules of engagement, etc.), is becoming the prelude to future planning and response to potentially offensive cyber warfare actions (e.g., those that fall under the concept of Offensive Operations in the Cyberspace (OOC)).

Resumen

I Introducción y motivación

Sin duda alguna, la importancia de los sistemas de Tecnologías de la Información y las Comunicaciones (TIC) está alcanzando picos nunca antes vistos. Es decir, las infraestructuras actuales de red se encuentran en una expansión constante, tanto en tamaño como en valor, con el objetivo último de proporcionar servicios útiles para los usuarios finales. Las consecuencias de esta expansión tienen un reflejo directo en nuestra vida cotidiana: miles de millones de personas están dispuestas a consumir esos servicios que han sido creados para mejorar su calidad de vida en general, tanto desde una perspectiva personal como profesional. Y dicha demanda es atendida por una multitud de dispositivos, que crecen en cantidad y ubicuidad. En concreto, estudios recientes indican que el número de dispositivos conectados a Internet sea de 20.000 millones, superando entre tres y cinco veces el número de personas conectadas a dicha red [1]. Por lo tanto, no debe sorprender que los individuos sean cada vez más dependientes de la tecnología. Además, el nuevo avance de las plataformas fifth-generation (5G) y beyond 5G (B5G) impulsa aún más esa revolución digital. De hecho, gracias a esas plataformas, la conectividad es capaz de alcanzar una velocidad asombrosa con una latencia increíblemente baja. Además, el auge de las tecnologías disruptivas (por ejemplo, Blockchain [2]) y de los paradigmas (por ejemplo, Internet de las Cosas (IoT por su sigla en inglés) [3]) ha allanado el camino a contribuciones destacables tanto del mundo industrial como de la investigación.

Sin embargo, la revolución digital no se desarrolla a coste cero. En efecto, a menudo se descuida la seguridad de los productos o servicios prestados, ya que el tiempo de comercialización es cada vez más corto debido a la mayor demanda [4]. Desencadenado por el alto beneficio potencial de la ciberdelincuencia, el número de actores con intenciones maliciosas ha aumentado significativamente durante los últimos años. Dichos delincuentes intentan realizar acciones dañinas contra los sistemas TIC de todo el mundo para perturbar los atributos de confidencialidad, integridad, y disponibilidad de dichos sistemas [5], afectando negativamente a los servicios prestados y comprometiendo la información relacionada con los mismos. Además, al aprovechar millones de dispositivos de todo el mundo, los atacantes son capaces de reclutar un ejército de máquinas para lanzar ofensivas de denegación de servicio distribuidos sin precedentes, devastando con relativa facilidad centros de datos enteros de última generación [6]. Sin embargo, las motivaciones de esos atacantes cambiaron con los años. A medida que los sistemas TIC iban aumentando, al principio los atacantes eran mayoritariamente individuos expertos que realizaban sus ac-

ciones maliciosas sólo para demostrar sus habilidades. Hoy en día, pueden ser descritos como auténticos grupos militarizados de personas con objetivos malévolos que a menudo venden sus destrezas perniciosas al mejor postor [7]. En este sentido, muchos de los ataques que se lanzan hoy en día son increíblemente sofisticados, implicando con frecuencia a los organismos de defensa de los estados en esta batalla sin fin [8]. Es decir, el concepto de ciber guerra se ha convertido recientemente en un asunto crucial a tratar por las naciones, ya que ahora el campo de batalla incluye también el ciberespacio [9].

En un contexto tan alarmante como éste, resulta fácil ver que la ciberseguridad y la ciberdefensa desempeñan un papel vital a la hora de blindar los dispositivos hiperconectados y proteger el ciberespacio. Sin embargo, luchar contra los incidentes ofensivos representa una tarea especialmente complicada debido a la naturaleza intrínsecamente dinámica de los sistemas TIC y a la diversidad de los potenciales vectores de ataque. En concreto, cada día se notifican vulnerabilidades críticas de nivel medio-alto que afectan a una inmensa cantidad de activos de sistemas diferentes [10]. Además, el tamaño de las infraestructuras mencionadas anteriormente genera dependencias difícilmente manejables entre los activos y servicios, que los atacantes pueden aprovechar para ejecutar ataques multi-paso hasta alcanzar su objetivo final [11]. En el contexto de esta Tesis Doctoral, la responsabilidad global de la ciberseguridad se ha desglosado en cuatro tareas principales, que están fuertemente conectadas ya que cada una de ellas proporciona información a la siguiente, construyendo un ciclo de protección:

- **Prevención**: la fase de prevención se encarga de supervisar continuamente el sistema subyacente para descubrir cualquier fallo de seguridad (por ejemplo, vulnerabilidades o configuraciones erróneas) y aplicar medidas de seguridad para solucionarlo.

- **Detección**: asumiendo que el sistema vigilado es (o será) vulnerable a posibles amenazas, la fase de detección se encarga de identificar con precisión y notificar con celeridad los incidentes intrusivos que suponen la explotación de fallos de seguridad.

- **Reacción**: una vez que se ha notificado un incidente, la reacción debe activarse para mitigar o incluso erradicar el ciber ataque, evaluando también el impacto del incidente y las consecuencias de las contramedidas. En particular, esta Tesis Doctoral se centrará en esta fase específica.

- **Análisis forense**: una vez que el incidente ha sido eliminado del sistema, el análisis forense necesita investigar las acciones registradas durante las fases anteriores. Esta operación permite descubrir aquello que salió mal para así evitar episodios similares en el futuro.

Entre esas fases, la reacción puede describirse como un paso fundamental en la interminable carrera armamentística entre los bandos ofensivos y defensivos. Normalmente, la reacción tiene un doble objetivo: por un lado, debe seleccionar el conjunto óptimo de contramedidas para bloquear inmediatamente la amenaza en curso [12]. Por otro lado, debe indicar el conjunto de acciones para restablecer el sistema y devolverlo a un estado operativo normal [13]. Sorprendentemente, la etapa de reacción ha recibido bastante menos atención tanto por parte de la academia como de la industria con respecto a la detección. Las principales razones de este desequilibrio podrían atribuirse a los diversos retos que confluyen en el ecosistema de la reacción, los cuales han sido analizados y abordados en el contexto de esta Tesis Doctoral. En este sentido, cabe destacar la función crucial que desempeñan los administradores de seguridad del sistema. Concretamente, estos se encargan de seleccionar las acciones más adecuadas en cada una de las fases de ciberseguridad

antes mencionadas. En lo que respecta a la fase de reacción, los administradores de seguridad soportan la carga encontrar el equilibrio óptimo entre la eficacia de la respuesta y su potencial impacto negativo en los activos del sistema, trabajando siempre con estrictas limitaciones presupuestarias [14]. En un mundo digital que avanza hacia la completa automatización de los procesos (incluidos los de seguridad), esta Tesis destaca el papel central de los administradores de seguridad en cada estrategia de reacción, siendo quienes en última instancia toman las decisiones aprovechando su experiencia en ciberseguridad.

Además, a lo largo de esta Tesis Doctoral, otro concepto esencial es la diferencia entre los dos enfoques primarios de la reacción, concretamente, el estático y el dinámico:

- **Reacción estática**: esta respuesta se encarga de trabajar proactivamente contra posibles incidentes de seguridad. Principalmente, se ocupa de identificar las características del sistema con especial atención a las debilidades, vulnerabilidades y configuraciones incorrectas. Esta tarea deriva en una correcta estimación del riesgo, pero no suele ser trivial debido a la complejidad y el tamaño de los sistemas a proteger.
- **Reacción dinámica**: este enfoque se encarga de contrarrestar los posibles ataques en curso. En este caso, además de un conocimiento holístico del sistema, es fundamental la evaluación de los objetivos del atacante y el tiempo de respuesta, entre otros aspectos.

En este sentido, está claro que la reacción dinámica requiere más potencia de cálculo, y las selecciones de contramedidas deben hacerse equilibrando la relación coste-beneficio en tiempo casi real. Así, la escalabilidad de las soluciones dinámicas propuestas en la literatura tiende a ser inadecuada, lo que se refleja en los reducidos entornos de prueba propuestos por los distintos autores de dichas soluciones. Además, los trabajos de reacción no adoptan una metodología de evaluación estándar para proporcionar un análisis cuantitativo de la estrategia de defensa que proponen. Se podría decir, por tanto, que es necesario un modelo estándar que pueda evaluar el equilibrio entre el impacto del ataque y el coste de la defensa a la hora de aplicar las contramedidas para cada esquema de reacción. Además, la lucha contra los ciberataques debe basarse en un conocimiento exhaustivo y común de las contramedidas. De hecho, las metodologías de reacción presentadas en la literatura proponen aplicar contramedidas *ad-hoc*, que a menudo se basan en las opiniones subjetivas de los autores.

II Objetivos

El objetivo principal de esta Tesis Doctoral consiste en estudiar, analizar y abordar las principales limitaciones de los sistemas de reacción del estado del arte, lo que conduce al desarrollo de un sistema de selección de contramedidas escalable y robusto, que pueda calcular la reacción óptima a partir de una alerta de seguridad o cualquier procedimiento de descubrimiento de fallos de seguridad. Además, dicha reacción debería basarse en una representación de contramedidas común y compartida que aproveche el conocimiento exhaustivo de dichas contramedidas.

Más concretamente, el objetivo principal puede dividirse en varios subobjetivos, que se listan a continuación:

1. Analizar las propuestas actuales del estado del arte sobre el ecosistema de reacción.
2. Identificar las principales ventajas e inconvenientes potenciales de los sistemas de reacción estudiados.

3. Analizar los retos actuales de este campo para trazar las direcciones de la investigación futura.

4. Proponer una representación estándar de los objetos de contramedidas.

5. Estudiar la viabilidad de la propuesta de contramedidas estándar en diferentes escenarios de casos reales.

6. Introducir un índice para evaluar el beneficio de la aplicación de una o varias contramedidas sobre el mismo activo, considerando la eficacia, el impacto negativo y el coste.

7. Presentar una metodología de reacción novedosa y robusta para seleccionar el conjunto óptimo de contramedidas.

8. Evaluar el rendimiento de la metodología sugerida a través de experimentos exhaustivos.

III Metodología

Dado que esta Tesis Doctoral fue concebida desde su inicio como un compendio de publicaciones, todo el trabajo realizado a lo largo de la trayectoria del doctorado estuvo orientado a la consecución de este objetivo. Cabe destacar que la Tesis Doctoral está co-supervisada y co-financiada por Indra[1], empresa internacional que integró algunos de los resultados de investigación de este trabajo en su cartera de productos y soluciones para la ciberdefensa. En consecuencia, los objetivos de la Tesis Doctoral descritos en el apartado anterior han sido consensuados entre la Universidad de Murcia e Indra para asegurar el completo alineamiento entre los objetivos científicos y las necesidades de la empresa.

Indra es un proveedor líder de soluciones para el sector de la defensa, que ha identificado la reacción dinámica contra las ciberamenazas como base para reforzar sus productos de ciberconsciencia situacional. En concreto, la fase de reacción supone un área estratégica en su actividad principal para el mercado de la defensa, donde ya se están invirtiendo recursos esenciales para desarrollar una nueva cartera de productos de ciberdefensa en torno a las capacidades relacionadas con el conocimiento de la situación cibernética. Algunas de las partes interesadas a las que se dirigen los resultados de la Tesis Doctoral son los Ministros de Defensa Nacionales, la Agencia Europea de Defensa (EDA, por sus siglas en inglés de "*European Defence Agency*"), la Cooperación Estructurada Permanente (PESCO, por sus siglas en inglés de "*Permanent Structured Cooperation*"), o la Organización del Tratado del Atlántico Norte (OTAN). En este sentido, esta Tesis Doctoral posee un valor añadido que Indra espera explotar comercialmente poco después de que los resultados de la Tesis Doctoral hayan entrado en producción.

III.1 Estudio de los sistemas de reacción

El primer hito de esta Tesis Doctoral tiene que ver con el estudio del estado del arte de los sistema de reacción, al que se hace referencia en su primer capítulo (A Comprehensive Survey on Reaction Frameworks (Article 1–IEEECOMST)). Recoger, estudiar y analizar los principales trabajos relevantes en el ecosistema de las reacciones representa sin duda un paso fundamental. En efecto, permite identificar los retos del campo para así trazar las futuras líneas de investigación. Concretamente, el estudio incluye los 24 trabajos más

[1] `https://www.indracompany.com`

notables publicados en los últimos 5 años (es decir, de 2012 a 2016) que tratan de la reacción contra los ciberataques. Dicho estudio tiene un doble objetivo: en primer lugar, pretende analizar en profundidad las propuestas significativas en este campo. En segundo lugar, ofrece un análisis exhaustivo y una comparación entre los trabajos seleccionados en función de siete criterios comunes. En concreto, los criterios utilizados en la comparativa son:

- **Modelado de ataques**: un modelo formal para describir las acciones de los posibles atacantes centrándose en los fallos de seguridad presentes en el sistema protegido.
- **Técnica de provisión de contramedidas**: la metodología (y las métricas relacionadas) para seleccionar y aplicar un conjunto de contramedidas sobre los activos del sistema.
- **Evaluación de los resultados**: la evaluación del resultado de los trabajos analizados, es decir, la provisión de acciones de remediación. En particular, se extraen dos características, concretamente, el banco de pruebas y el papel del administrador.
- **Tipo de reacción**: la reacción se contempla siguiendo dos enfoques principales, concretamente, la reacción estática y la dinámica, como ya se ha mencionado.
- **Uso de estándares**: el uso de estándares en el diseño, desarrollo y evaluación de las estrategias de reacción facilita la comparación entre los trabajos y soluciones publicados, dando una medida cuantitativa y cualitativa de su eficacia.
- **Nivel de automatización**: debido a la potencial complejidad del marco de reacción, el nivel de automatización se considera un factor esencial.
- **Rendimiento**: se recogen y detallan los factores que inciden fuertemente en la aplicación de la estrategia de contramedidas.

En la Figura 1 se muestra un resumen gráfico de los trabajos estudiados según el año de publicación y sus principales características. En particular, dicha figura repasa la evolución del tema de investigación analizado, en el que los autores aportan diferentes propuestas de reacción contra los ciberataques. A continuación, se destacan los aspectos positivos y negativos de cada trabajo.

A partir del análisis en profundidad realizado, se identificaron seis retos de investigación que parecen ser los más destacados en el desarrollo de una solución de reacción:

- **Escalabilidad**: uno de los principales inconvenientes de los trabajos estudiados es la escasa escalabilidad. En concreto, se reconoce que el modelado de los ataques es la principal causa de dicha deficiencia.
- **Conocimiento de contramedidas**: cada una de las propuestas estudiadas utilizaba sólo un conjunto reducido de contramedidas aplicadas sobre los activos contra ataques específicos.
- **Representación estándar**: otra carencia surgida durante el estudio consiste en la ausencia de una representación estándar de la contramedida.
- **Correlación contramedidas-ataques**: una vez que se ha construido un conjunto completo de contramedidas, el análisis minucioso de la correlación entre las contramedidas y los ataques también representa una necesidad primordial.

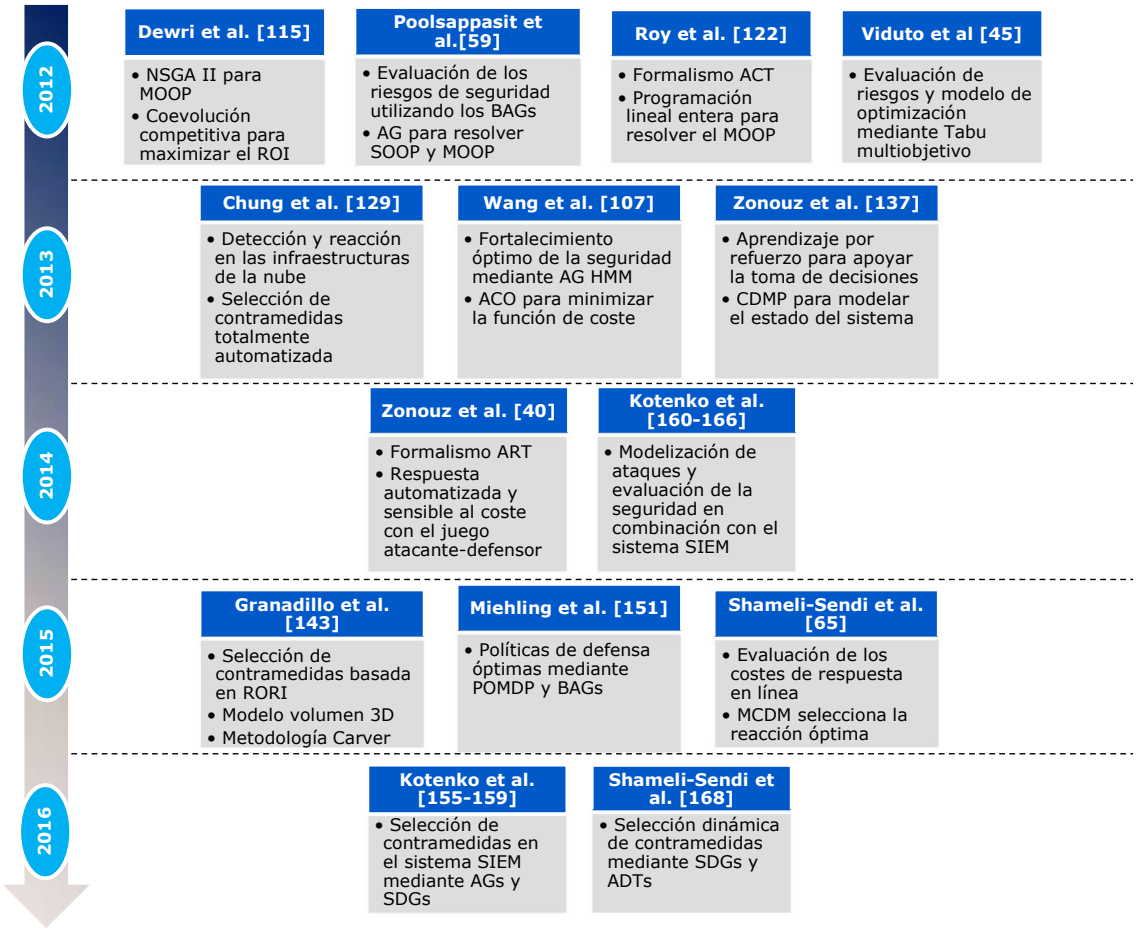


Figura 1: Cronología de las publicaciones estudiadas, destacando su novedad y sus características principales.

- **Métricas y sistemas de puntuación**: entre los trabajos analizados se ha encontrado una ausencia destacable de un sistema de medición específico y de uso común para analizar cuantitativamente las propuestas de reacción.
- **Mitigación de ataques de día cero**: la gran mayoría de las estrategias de contramedidas presentadas descuidan la reacción contra incidentes ofensivos desconocidos.

Para cada una de ellas, se han propuesto varias soluciones que pueden contribuir a esta importante área de investigación.

III.2 Propuesta de contramedidas estándar

Partiendo de los retos destacados en el estudio anterior, otro logro significativo de esta Tesis Doctoral es la propuesta de una representación estándar de una contramedida, detallando con granularidad fina los campos que son necesarios para abarcar el objeto de remediación. Como se detalla en el segundo capítulo (Towards Pre-standardization of Countermeasures (Article 2–`Clus`)), dicha representación sirve como punto de partida hacia la estandarización de las contramedidas dentro del ecosistema de la reacción, permitiendo el intercambio continuo de conocimientos sobre la reacción entre los equipos de seguridad

de todo el mundo. Además, una representación estándar de los objetos de remediación sirve de base para construir estrategias de reacción robustas, constantemente refrescadas con nuevas instancias.

La representación propuesta tiene en cuenta las características específicas de cada contramedida (por ejemplo, la eficacia, el impacto, el coste, o los posibles parámetros), pero también aprovecha el conocimiento de seguridad que ya está presente en otros repositorios de seguridad ampliamente utilizados (por ejemplo, bases de conocimiento de plataformas, ataques, vulnerabilidades, o configuraciones). En este sentido, la reutilización de conocimientos de seguridad ya maduros y compartidos representa en última instancia un indicador importante para adoptar un formato estándar también para las contramedidas.

$$cm_{ID} = (\underbrace{ID, \mathit{Eff}, \mathit{Imp}, \mathit{Cost}, \Omega_c, \Omega_p, \Omega_v, \Omega_a, \phi}_{obligatorio}, \underbrace{P, \delta}_{opcional}) \tag{1}$$

Más concretamente, la definición propuesta se representa en la ecuación 1, mientras que sus componentes se detallan a continuación:

- $ID \in \mathbb{N}$ es el identificador unívoco de la contramedida.
- $\mathit{Eff} \in \{L, M, H, X\}$ representa la eficacia residual de la contramedida, refiriéndose a su capacidad para bloquear la amenaza.
- $\mathit{Imp} \in \{L, M, H, X\}$ se refiere al impacto residual de la contramedida, ya que puede afectar negativamente a los activos correspondientes dentro del sistema monitorizado.
- $\mathit{Cost} \in \mathbb{R}^+$ representa el coste residual de la contramedida, que contempla el despliegue, el mantenimiento y los costes indirectos.
- $\Omega_c = \{c_i \in C\}$ es el enlace a la base de conocimientos de configuración común C a la que se refiere el activo designado.
- $\Omega_p = \{p_i \in P\}$ es el enlace a la base de conocimientos de plataformas común P a la que se refiere el activo designado.
- $\Omega_v = \{v_i \in V\}$ es el enlace a la base de conocimientos de vulnerabilidades común V a la que se refiere la vulnerabilidad explotada.
- $\Omega_a = \{a_i \in A\}$ es el enlace a la base de conocimientos de ataques común A que la contramedida contrarresta.
- ϕ describe la aplicación de la contramedida en un formato legible para una máquina.
- $P = \{p_1, p_2, ..., p_n\}$, con $n \geq 0$, describe los parámetros que puede necesitar una determinada contramedida para ser aplicada.
- δ incluye información adicional sobre la contramedida, en particular:
  - una descripción textual, en lenguaje comprensible para el ser humano.
  - un campo que indica si el despliegue de la contramedida exige cambios de software o hardware.
  - una casilla que especifica si la contramedida es estática o dinámica.
  - un campo que exprese si la contramedida es de corta o larga duración dentro de la estrategia de reacción.

- ejemplos de la aplicación (por ejemplo, en pseudocódigo).
- si se aplica para la ciberdefensa, vinculación con las decisiones militares tácticas, estratégicas u operativas.

En el contexto de esta investigación, se utiliza un conjunto de valores discretos para evaluar la eficacia y el impacto residual de las contramedidas, a saber, L (Low, Bajo en español), M (Medium, Medio en español), H (High, Alto en español) y X (Undefined, No definido en español). En concreto, la representación propuesta aprovecha tanto los campos obligatorios como los opcionales. Los primeros se consideran rigurosamente necesarios para englobar correctamente las características esenciales de una contramedida, mientras que los segundos se presentan para caracterizar aún más dicha contramedida, no siendo cruciales para su representación o implementación. Sin embargo, cada uno de los campos sugeridos se describe con el detalle adecuado, discutiendo la razón principal de su elección dentro de la representación.

Además, para demostrar la aplicabilidad del enfoque, se presentan ejemplos de aplicación de contramedidas en escenarios reales. En particular, se presentan un escenario de *smart home*, un escenario de red empresarial y un escenario de infraestructura industrial. Aprovechando la representación propuesta, se demuestra la viabilidad de los objetos de contramedidas y aplican correctamente en los escenarios planteados, siendo eficaces contra las amenazas activas y protegiendo los activos del sistema.

Por último, se elabora un análisis en profundidad sobre la representación estándar propuesta, estudiando las características clave y las posibles mejoras hacia una estrategia de contramedidas completa.

III.3 Reacción impulsada por el SIA

Por su parte, otro logro destacable de esta Tesis Doctoral consiste en el diseño e implementación de una metodología novedosa y escalable para calcular el conjunto óptimo de contramedidas contra las ciberintrusiones, tal y como se describe en el tercer capítulo de este documento (AIS-powered Optimal Countermeasures Selection (Article 3–`IEEEAccess`)). Dicha solución aprovecha las extraordinarias capacidades de un Sistema Inmunológico Artificial (SIA). Esta técnica bioinspirada es capaz de calcular resultados óptimos en un tiempo más que aceptable gracias a las continuas fases de clonación y mutación. Además, las contramedidas se encapsulan en la representación estándar propuesta, reforzando la interoperabilidad de las estrategias de reacción.

Específicamente, se realiza una fase de modelado preliminar para trasladar los conceptos relacionados con la inmunidad del SIA al contexto de reacción de la ciberseguridad. En este sentido, los activos $A_x \in A$ son el foco principal del proceso de reacción. En todo momento, esos activos exigen protección contra las posibles amenazas $\tau_k \in T$, es decir, vulnerabilidades y ataques, minimizando el riesgo al que están expuestos. En este sentido, las amenazas T representan los *antígenos* contra los que la reacción del SIA calcula la respuesta óptima mediante *anticuerpos*, es decir, el conjunto de contramedidas CM.

Para calcular las contramedidas atómicas $cm_i \in CM$ que pertenecen a la solución óptima, se propone el beneficio de la contramedida $B(cm_i)$. Este índice contempla las ventajas de aplicar pasos de reacción específicos sobre un determinado activo equilibrando el compromiso entre su eficacia y su impacto negativo y coste. A continuación, el modelo se enriquece considerando la posibilidad de aplicar un conjunto de contramedidas sobre un activo concreto de forma simultánea.

Tras una profunda fase de modelización, se describe la reacción impulsada por el SIA para minimizar la diferencia entre el riesgo al que están expuestos los activos (es decir, el

riesgo medido $RL(\tau_k, A_x)$) y el nivel de riesgo aceptable asignado a cada activo $\widetilde{RL}(A_x)$ aplicando un conjunto de contramedidas $CM_j(A_x)$. Concretamente, la reacción impulsada por el SIA es capaz de determinar el conjunto óptimo de contramedidas atómicas mediante la clonación y mutación continuas de los anticuerpos dentro del espacio de la solución.

La Figura 2 ilustra un ejemplo de los pasos de la reacción impulsada por el SIA. En primer lugar, se genera aleatoriamente un conjunto inicial de anticuerpos (es decir, un conjunto de contramedidas atómicas). En el ejemplo propuesto, $\mathbb{CM} = \{CM_1, CM_2, CM_3\}$. A continuación, se calcula la afinidad de los anticuerpos generados, es decir, se mide la capacidad de reducir la diferencia entre el riesgo medido y aceptable. Suponiendo que el mejor anticuerpo sea CM_1 y el factor de clonación $K = 1$, dicho anticuerpo se clona y, sucesivamente, se muta. Suponiendo que la afinidad del clon CM_1' sigue siendo mejor que la afinidad media, éste se incluye en el espacio de la solución $\mathbb{CM}$ sustituyendo al peor anticuerpo, por ejemplo, CM_3. Finalmente, el peor anticuerpo restante dentro de $\mathbb{CM}$, por ejemplo, CM_2, se sustituye por uno generado aleatoriamente para iniciar otra iteración de la reacción SIA.

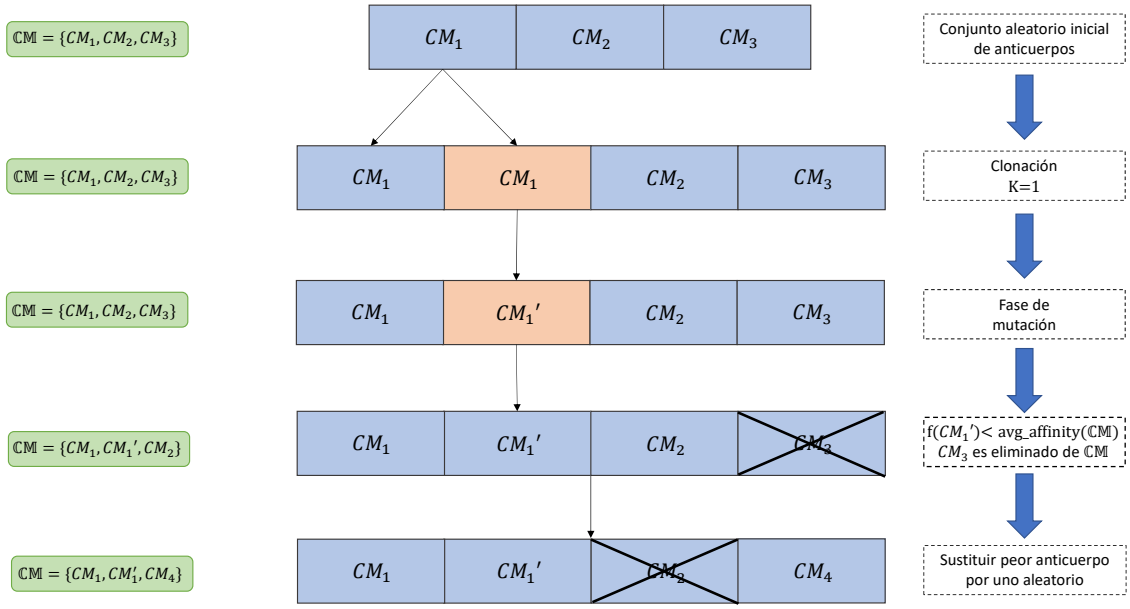


Figura 2: Pasos de la reacción impulsados por el SIA.

A continuación, se presentan versiones estáticas y dinámicas de las reacciones impulsadas por el SIA, en función de la fase en la que se dispara el procedimiento. Además, se sugiere una condición de terminación sensible al contexto que, basándose en el fitness inicial observado, asigna valores específicos a los parámetros de entrada del procedimiento para calcular soluciones rápidamente cuando el fitness inicial es alto (es decir, los activos están expuestos a una situación de alto riesgo), mientras que computa durante más tiempo buscando mejores soluciones cuando el fitness inicial es bajo.

Además, la metodología propuesta se ha sometido a una intensa batería de experimentos, en la que los parámetros de los escenarios subyacentes (es decir, las amenazas, los activos y las contramedidas) se han generado aleatoriamente para argumentar mejor las capacidades de la metodología mediante la introducción de la aleatoriedad. En este sentido, los experimentos demuestran las capacidades y la robustez del procedimiento, ayudando a los actores humanos en el procedimiento de toma de decisiones.

IV Otras publicaciones relevantes

Además, durante su Tesis Doctoral, el doctorando también ha participado en varios proyectos de investigación relacionados con aspectos de ciberseguridad, dando lugar a las correspondientes publicaciones que han enriquecido sus habilidades tanto desde la perspectiva de la investigación como del trabajo en equipo. A continuación, las publicaciones se agrupan en función del proyecto de investigación o colaboración al que están vinculadas.

IV.1 Despliegue de una solución SIEM para la protección de los activos de información

En este proyecto se revisan las condiciones de seguridad de los dispositivos IoT para proponer una arquitectura de ciberseguridad para los sistemas IoT que implique un paradigma de seguridad holístico para la protección de los activos de información. Dicha solución debe ser fácil de seguir por los desarrolladores de tecnología, las áreas TIC y los usuarios, fortaleciendo así los entornos tecnológicos de las organizaciones, así como los individuos que los utilizan.

Este proyecto se ha llevado a cabo junto con la Escuela Colombiana de Ingeniería "Julio Garavito", de Bogotá, Colombia, resultando en una interesante colaboración internacional y una visita muy fructífera a Bogotá en diciembre de 2017. A continuación se enumeran los artículos publicados, indicando en el caso de las publicaciones en revistas su *Journal Impact Factor* (JIF), así como el cuartil al que pertenecen (Q1, Q2, Q3 o Q4):

- Daniel O. Díaz López, María Blanco Uribe, Claudia Santiago Cely, Andrés Vega Torres, Nicolás Moreno Guataquira, Stefany Moron Castro, Pantaleone Nespoli, Félix Gómez Mármol, "**Shielding IoT against cyber-attacks: An event-based approach using SIEM**.", *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–18, 2018.
  DOI: 10.1155/2018/3029638
  JIF 2018: 1.396 (Q3)

- Daniel O. Díaz López, Maria Blanco Uribe, Claudia P. Santiago Cely, Daniel F. Tarquino Murgueitio, Edwin S. García García, Pantaleone Nespoli, Félix Gómez Mármol, "**Developing secure IoT services? A security-oriented review of IoT platforms**.", *Symmetry*, vol. 10, pp. 1–34, 2018.
  DOI: 10.3390/sym10120669
  JIF 2018: 2.143 (Q2)

- Juan Velandia Botello, Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel O Díaz López, Pantaleone Nespoli, Félix Gómez Mármol, "**BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM**.", *Sensors, Special Issue on Blockchain Security and Privacy for the Internet of Things*, vol. 20, pp. 1–22, 2019.
  DOI: 10.3390/s20164636
  JIF 2019: 3.275 (Q1)

IV.2 COSMOS: Centinela colaborativo, transparente y adaptativo para el Internet de las Cosas

El proyecto COSMOS pretende desarrollar soluciones novedosas e innovadoras para proporcionar sofisticados mecanismos de protección a los dispositivos IoT. En concreto, su

principal objetivo es el desarrollo de los así llamados centinelas colaborativos, transparentes y adaptativos, que blindan automáticamente los dispositivos IoT circundantes contra posibles amenazas.

Este proyecto fue financiado por una Beca Leonardo concedida por la Fundación BBVA[2] y realizado en la Universidad de Murcia en colaboración con varios otros centros de investigación [3]. Las publicaciones relacionadas se enumeran a continuación:

- Pantaleone Nespoli, Félix Gómez Mármol, "**e-Health Wireless IDS with SIEM integration**.", *IEEE Wireless Communication and Networking Conference (WCNC 2018), Barcelona, Spain.*

- David E. Useche Peláez, Daniel O. Díaz López, Pantaleone Nespoli, Félix Gómez Mármol, "**TRIS: a Three-Rings IoT Sentinel to protect against cyber-threats**.", *Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2018), Valencia, Spain.*

- Pantaleone Nespoli, David E. Useche Peláez, Daniel O. Díaz López, Félix Gómez Mármol, "**COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things**.", *Sensors, Special Issue on Sensor Systems for Internet of Things*, vol. 19, pp. 1–29, 2019.
  DOI: 10.3390/s19071492
  JIF 2019: 3.275 (Q1)

- Pantaleone Nespoli, Daniel O. Díaz López, Félix Gómez Mármol, "**Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices**.", *Journal of Information Security and Applications, Special Issue on Cybersecurity Trends*, vol. 60, p. 102878, 2021.
  DOI: 10.1016/j.jisa.2021.102878
  JIF 2019: 2.327 (Q3)

IV.3 AUTHCODE: autenticación para el acceso continuo a los servicios

La autenticación continua en dispositivos móviles tiene como objetivo identificar al propietario (o propietarios) de un determinado dispositivo en cualquier momento. El principal beneficio de la autenticación continua consiste en mejorar la experiencia del usuario al utilizar servicios o aplicaciones en sus dispositivos móviles, evitando complejas credenciales de acceso.

Este proyecto fue financiado por la Fundación Séneca [4] y realizado en la Universidad de Murcia. A continuación se enumeran los artículos de investigación publicados:

- Pantaleone Nespoli, Mattia Zago, Alberto Huertas Celdrán, Manuel Gil Pérez, Félix Gómez Mármol, Félix J. García Clemente, "**A Dynamic Continuous Authentication Framework in IoT-Enabled Environments**.", *Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2018), Valencia, Spain.*

- Pantaleone Nespoli, Mattia Zago, Alberto Huertas Celdrán, Manuel Gil Pérez, Félix Gómez Mármol, Félix J. García Clemente, "**PALOT: Profiling and Authenticating users Leveraging internet Of Things**.", *Sensors, Special Issue on Sensor*

[2] https://www.fbbva.es/en/
[3] https://webs.um.es/felixgm/projects/cosmos/
[4] https://www.fseneca.es/

Systems for Internet of Things, vol 19, pp. 1–26, 2019.
DOI: 10.3390/s19122832
JIF 2019: 3.275 (Q1)

- Pedro M Sánchez Sánchez, José M Jorquera Valero, Mattia Zago, Alberto Huertas Celdrán, Lorenzo Fernández Maimó, Eduardo López Bernal, Sergio López Bernal, Javier Martínez Valverde, Pantaleone Nespoli, Javier Pastor Galindo, Ángel L Perales Gómez, Manuel Gil Pérez, Gregorio Martínez Pérez, "**BEHACOM-a dataset modelling users' behaviour in computers**.", *Data in Brief*, vol. 31, pp. 1–12, 2020.
  DOI: 10.1016/j.dib.2020.105767
  SJR. 2019: 0.105 (Q4)

IV.4 BotBusters: a la caza de bots en redes sociales

El proyecto BotBusters tiene como objetivo proporcionar soluciones de inteligencia artificial para concienciar a los usuarios de las actividades coordinadas de los bots sociales. Recientemente, se ha observado un aumento significativo de bots sociales con intención de manipular a la comunidad de las redes sociales. Los bots sociales constituyen hoy en día ejércitos controlados por malhechores que pretenden manipular y engañar a los usuarios de estos entornos y plataformas.

Este proyecto fue premiado como ganador regional en el Premio Ericsson a la Innovación 2018[5]. Fue creado en el marco de una colaboración de investigación entre estudiantes de la Universidad de Murcia (incluido el doctorando) y la Universidad del Mar Egeo (Grecia).

Las publicaciones relacionadas son las siguientes:

- Javier Pastor-Galindo, Pantaleone Nespoli, Félix Gómez Mármol, Gregorio Martínez Pérez, "**OSINT is the next Internet goldmine: Spain as an unexplored territory**.", *Fifth National Conference on Cybersecurity (JNIC 2019), Cáceres, Spain.*

- Mattia Zago, Pantaleone Nespoli, Dimitrios Papamartzivanos, Manuel Gil Pérez, Félix Gómez Mármol, Georgios Kambourakis, Gregorio Martínez Pérez, "**Screening out social bots interference: are there any silver bullet?**.", *IEEE Communications Magazine*, vol. 5, pp. 98–104, 2019.
  DOI: 10.1109/MCOM.2019.1800520
  JIF 2019: 11.052 (Q1)

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez Pérez, Félix Gómez Mármol, "**Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**.", *IEEE Transactions on Network and Service Management, Special Issue on Data Analytics and Machine Learning for Network and Service Management*, vol. 20, pp. 2156–2170, 2020.
  DOI: 10.1109/TNSM.2020.3031573
  JIF 2019: 3.878 (Q1)

- Javier Pastor-Galindo, Pantaleone Nespoli, Félix Gómez Mármol, Gregorio Martínez Pérez, "**The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends**.", *IEEE Access*, vol. 8, pp. 10282–10304, 2020.
  DOI: 10.1109/ACCESS.2020.2965257
  JIF 2019: 3.745 (Q1)

[5] https://bit.ly/2RZhYr8

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez Pérez, Félix Gómez Mármol, "**Twitter social bots: the 2019 Spanish general election data**.", *Data in Brief*, vol. 32, pp. 1–10, 2020.
  DOI: 10.1016/j.dib.2020.106047
  SJR 2019: 0.105 (Q4)

- Javier Pastor-Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, José A. Ruipérez Valiente, Alberto Huertas Celdrán, Manuel Gil Pérez, Gregorio Martínez Pérez, Félix Gómez Mármol, "**A Review of Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**.", *Sixth National Conference on Cybersecurity (JNIC 2021), Castilla-La Mancha, Spain.*

IV.5 COnVIDa: Recolección de datos multidisciplinares y panel de control de la COVID19

COnVIDa[6] es una herramienta web desarrollada por el Laboratorio de Ciberseguridad y Ciencia de Datos de la Universidad de Murcia[7] que recoge de forma eficiente los datos relacionados con la pandemia de COVID19 desde diferentes fuentes de datos en el contexto de España y los visualiza en un cuadro de mando. En este sentido, COnVIDa puede describirse como nuestra pequeña contribución a la batalla contra la pandemia.

A continuación se expone el principal artículo de investigación relacionado con este proyecto:

- Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Javier Pastor Galindo, Pantaleone Nespoli, Félix J. García Clemente, Félix Gómez Mármol. "**COnVIDa: COVID19 multidisciplinary data collection and dashboard**.", *Journal of Biomedical Informatics, Special Issue on Novel Informatics Approaches to COVID-19 Research*, vol. 117, p. 103760, 2021.
  DOI: 10.1016/j.jbi.2021.103760
  JIF 2019: 3.526 (Q2)

IV.6 COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación

Este proyecto tiene como objetivo desarrollar módulos hiperrealistas de simulación de Amenazas Persistentes Avanzadas (APTs) y topologías de red y tráfico que simulen escenarios realistas para ser integrados en Ciber Ranges, con un módulo que permita el desarrollo de escenarios de maniobras cibernéticas de plantillas parametrizables y aleatorias. El Cyber Range se integrará con elementos de gamificación y aprendizaje adaptativo para hacer el proceso de aprendizaje más motivador y adaptativo.

Este proyecto ha sido financiado por el Ministerio de Defensa español a través de la subvención 10032/20/0035/00.

Las publicaciones relacionadas se enumeran a continuación:

- Félix Gómez Mármol, José A. Ruipérez-Valiente, Pantaleone Nespoli, Gregorio Martínez Pérez,Diego Rivera Pinto, Xavier Larriva Novo, Manuel Álvarez-Campana, Víctor Villagrá González, Jorge Maestre Vidal, Francisco A. Rodriguez López, Miguel

[6] https://convida.inf.um.es/
[7] https://cyberdatalab.um.es/

Páramo Castrillo, Javier I. Rojo Lacal, Ramón García-Abril Alonso, "**COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación**.", *Sixth National Conference on Cybersecurity (JNIC 2021), Castilla-La Mancha, Spain.*

V Conclusiones y trabajo futuro

La revolución digital está ocurriendo ante nuestros ojos y está cambiando nuestras vidas. En efecto, los usuarios confían cada vez más en los servicios que ofrecen las infraestructuras de red actuales, creados para mejorar su calidad de vida. La extraordinaria hiperconectividad de los dispositivos y la forma en que los seres humanos pueden comunicarse entre sí eran simplemente increíbles hace sólo unos años.

Sin embargo, el amplio abanico de oportunidades y el importante crecimiento económico que ofrece esta revolución también conlleva consecuencias negativas. De hecho, también estamos asistiendo al surgimiento de organizaciones malintencionadas cuyo principal objetivo es golpear las infraestructuras de la red con fines económicos y estratégicos. Nadie queda excluido de esta interminable batalla: desde los ciudadanos hasta los gobiernos, los ciberdelincuentes amenazan sin piedad a entidades de todo el mundo.

En un escenario tan peligroso, los mecanismos de seguridad para proteger el ciberespacio son más necesarios que nunca. Es decir, la ciberseguridad y la ciberdefensa son esenciales para defender los sistemas TIC de los ciberataques. Entre las cuatro fases principales de la ciberdefensa (prevención, detección, reacción y análisis forense), la reacción contra los ciberataques puede describirse como crucial para erradicar dinámicamente las posibles amenazas dentro del sistema vigilado y, posteriormente, restablecer los activos relacionados. Sorprendentemente, la fase de reacción ha recibido bastante menos atención en comparación con las otras fases de ciberseguridad, principalmente debido a las dificultades a las que se enfrenta.

Con el objetivo de contribuir al ecosistema de las reacciones, esta Tesis Doctoral se centra en el análisis de los retos de este campo y en la propuesta de soluciones eficaces para los mismos. Teniendo en cuenta los objetivos enumerados en la Sección II, se han logrado las siguientes contribuciones principales:

i) en primer lugar, el estudio en profundidad de los sistemas de reacción del estado del arte. Dichas estrategias de respuesta se han comparado entre sí en base a siete criterios comunes, poniendo de manifiesto los retos que aún plantea este campo, tal y como se detalla en Article 1–`IEEECOMST`.

ii) en segundo lugar, la propuesta de una representación estándar de las contramedidas, con el objetivo de impulsar el intercambio de conocimientos sobre las reacciones entre los equipos de seguridad y construir planes de respuesta robustos, como se detalla en Article 2–`Clus`.

iii) en tercer lugar, el diseño y la implementación de un novedoso sistema de reacción que aprovecha las características más destacadas del SIA. La metodología propuesta es capaz de seleccionar el conjunto óptimo de contramedidas atómicas que se activan contra las amenazas identificadas dentro del sistema protegido de una manera eficaz y eficiente, como se describe en Article 3–`IEEEAccess`.

Dichas contribuciones han sido publicadas en revistas de primer nivel con el fin de difundir los resultados y alcanzar a la comunidad investigadora como objetivo final. Además,

los resultados han sido supervisados y compartidos con Indra, con el objetivo de explotarlos en sus actividades principales para el mercado de la defensa.

Sin embargo, aún queda mucho camino por recorrer en la carrera armamentística entre las estrategias de reacción y los ciberdelincuentes. De hecho, algunos retos parecen estar aún sin resolver y requerirán importantes contribuciones en el futuro.

En concreto, es evidente la falta de un sistema de evaluación de contramedidas comúnmente utilizado y compartido. Hasta ahora, se han propuesto varios índices en la literatura, tratando de capturar diferentes aspectos de las medidas de corrección. Sin embargo, la creación de un sistema de puntuación de contramedidas estándar, aprovechando otros esquemas de evaluación existentes, sería muy beneficiosa para cada estrategia de reacción, ya que sus resultados podrían compararse con mayor equidad. En este sentido, la propuesta de representación estándar de contramedidas se ha de considerar un punto de partida hacia este objetivo.

Además, la metodología de reacción diseñada, impulsada por el SIA, ha sido probada mediante la simulación del sistema monitorizado subyacente durante los experimentos. En este sentido, se podría decir que sería interesante emplear la metodología propuesta en un escenario de uso real, estudiando la viabilidad de la aplicación de la reacción SIA con tráfico de red real, desde la detección de la amenaza hasta la ejecución de la contramedida. Este flujo de información de seguridad se beneficiaría sin duda de la utilización de un modelo de ataque (por ejemplo, grafo de ataque, árbol de ataque, etc.) para predecir los movimientos y objetivos de los atacantes. Posiblemente, un marco de detección-reacción tan completo requerirá los esfuerzos conjuntos de diferentes instituciones de investigación, lo que encajará en el contexto de una potente propuesta de proyecto de investigación. Asimismo, se considera de gran interés un método de meta-optimización para mejorar la selección de la respuesta del SIA. En esta dirección, el doctorando está trabajando actualmente en la propuesta de una metodología evolutiva (es decir, Algoritmo Genético) para optimizar dichos parámetros y probar la robustez de la reacción impulsada por el SIA.

Por último, pero no por ello menos importante, el análisis del enriquecimiento de las estrategias de reacción con contramedidas ofensivas es un tema digno de estudio. Concretamente, debido a la colaboración altamente fructífera con Indra, que cuenta con varios clientes militares en su cartera, la posibilidad de estudiar, analizar e implementar contramedidas ofensivas representa una interesante línea de trabajo futura. Por ejemplo, este es un tema de gran interés para la Plataforma Europea de Consciencia Situacional en el Ciberespacio (ECYSAP, del inglés *European Cyber Situational Awareness Platform*), cuyo desarrollo lidera Indra. En este contexto, la capacidad de dar una respuesta activa a ciberamenazas, que sea proporcional y aceptable tanto en términos tecnológicos como regulatorios (doctrina, marco ético, legislación, reglas de compromiso, etc.), se está convirtiendo en la antesala para la futura planificación y respuesta ante acciones de ciber guerra potencialmente ofensivas (por ejemplo, aquellas que se enmarcan en el concepto de las Operaciones Ofensivas en el Ciberespacio (OOC)).

Bibliography

[1] D. Goad, A. T. Collins, and U. Gal, "Privacy and the internet of things : An experiment in discrete choice," *Information & Management*, vol. 58, no. 2, p. 103292, 2021. DOI: 10.1016/j.im.2020.103292

[2] J. V. Botello, A. P. Mesa, F. A. Rodríguez, D. Díaz-López, P. Nespoli, and F. G. Mármol, "BlockSIEM: Protecting smart city services through a Blockchain-based and distributed SIEM," *Sensors*, vol. 20, no. 16, 2020. DOI: 10.3390/s20164636

[3] P. Nespoli, D. Useche Peláez, D. Díaz López, and F. Gómez Mármol, "COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things," *Sensors*, vol. 19, no. 7, 2019. DOI: 10.3390/s19071492

[4] D. Geer, E. Jardine, and E. Leverett, "On market concentration and cybersecurity risk," *Journal of Cyber Policy*, vol. 5, no. 1, pp. 9–29, 2020. DOI: 10.1080/23738871.2020.1728355

[5] A. A. Mishra, K. Surve, U. Patidar, and R. K. Rambola, "Effectiveness of confidentiality, integrity and availability in the security of cloud computing: A review," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 2018, pp. 1–5. DOI: 10.1109/CCAA.2018.8777537

[6] J. T. Martínez Garre, M. Gil Pérez, and A. Ruiz-Martínez, "A novel machine learning-based approach for the detection of ssh botnet infection," *Future Generation Computer Systems*, vol. 115, pp. 387–396, 2021. DOI: 10.1016/j.future.2020.09.004

[7] J. Maestre Vidal, M. A. Sotelo Monge, S. M. Martínez Monterrubio, L. I. Barona López, and A. L. Valdivieso Caraguay, "Profits at the dawn of cybercrime-as-a-service," in *2019 International Conference on Information Systems and Software Technologies (ICI2ST)*, 2019, pp. 71–78. DOI: 10.1109/ICI2ST.2019.00017

[8] D. S. Reveron and J. E. Savage, "Cybersecurity convergence: Digital human and national security," *Orbis*, vol. 64, no. 4, pp. 555–570, 2020. DOI: 10.1016/j.orbis.2020.08.005

[9] J. F. Lancelot, "Cyber-diplomacy: cyberwarfare and the rules of engagement," *Journal of Cyber Security Technology*, vol. 4, no. 4, pp. 240–254, 2020. DOI: 10.1080/23742917.2020.1798155

[10] M. A. Williams, R. C. Barranco, S. M. Naim, S. Dey, M. Shahriar Hossain, and M. Akbar, "A vulnerability analysis and prediction framework," *Computers & Security*, vol. 92, p. 101751, 2020. DOI: 10.1016/j.cose.2020.101751

[11] A. Shameli-Sendi, M. Dagenais, and L. Wang, "Realtime intrusion risk assessment model based on attack and service dependency graphs," *Computer Communications*, vol. 116, pp. 253–272, 2018. DOI: 10.1016/j.comcom.2017.12.003

[12] G. Gonzalez-Granadillo, E. Doynikova, J. Garcia-Alfaro, I. Kotenko, and A. Fedorchenko, "Stateful rori-based countermeasure selection using hypergraphs," *Journal of Information Security and Applications*, vol. 54, p. 102562, 2020. DOI: 10.1016/j.jisa.2020.102562

[13] G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, and H. Debar, "Dynamic risk management response system to handle cyber threats," *Future Generation Computer Systems*, vol. 83, pp. 535–552, 2018. DOI: 10.1016/j.future.2017.05.043

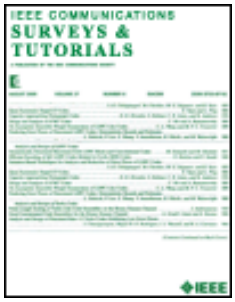
[14] F. Li, Y. Li, S. Leng, Y. Guo, K. Geng, Z. Wang, and L. Fang, "Dynamic countermeasures selection for multi-path attacks," *Computers & Security*, vol. 97, p. 101927, 2020. DOI: 10.1016/j.cose.2020.101927

Publications composing

the PhD Thesis

1

A Comprehensive Survey on Reaction Frameworks



Title:	Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks
Authors:	Pantaleone Nespoli, Dimitrios Papamartzivanos, Félix Gómez Mármol, Georgios Kambourakis
Journal:	IEEE Communication Surveys & Tutorials
JIF:	22.973 Q1
Publisher:	IEEE
Volume:	20
Pages:	1361–1396
Year:	2018
Month:	Secondquarter
DOI:	10.1109/COMST.2017.2781126
Status:	Published

Abstract

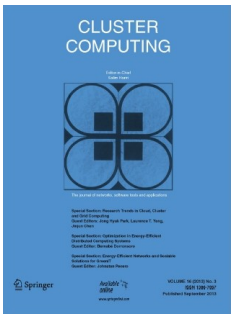
It is without doubt that today the volume and sophistication of cyber attacks keeps consistently growing, militating an endless arm race between attackers and defenders. In this context, full-fledged frameworks, methodologies, or strategies that are able to offer optimal or near-optimal reaction in terms of countermeasure selection, preferably in a fully or semi-automated way, are of high demand. This is reflected in the literature, which encompasses a significant number of major works on this topic spanning over a time period of 5 years, that is, from 2012 to 2016. The survey at hand has a dual aim, namely, first, to critically analyze all the pertinent works in this field, and second to offer an in-depth discussion and side-by-side comparison among them based on seven common criteria. Also, a quite extensive discussion is offered to highlight on the shortcomings and future research challenges and directions in this timely area.

Keywords

Cyber attack countermeasures · security risk assessment · Intrusion prevention and response systems · Decision support systems · Optimal countermeasure strategy · Dynamic reaction selection.

2

Towards Pre-standardization of Countermeasures



Title:	Battling against cyberattacks: Towards pre-standardization of countermeasures
Authors:	Pantaleone Nespoli, Félix Gómez Mármol, Jorge Maestre Vidal
Journal:	Cluster Computing
JIF:	3.458 Q1 (2019)
Publisher:	Springer
Volume:	24
Pages:	57–81
Year:	2021
Month:	Mar
DOI:	10.1007/s10586-020-03198-9
Status:	Published

Abstract

Cyberattacks targeting ICT systems are becoming every day more sophisticated and disruptive. Such malevolent actions are performed by ill-motivated entities (governments, states, administrations, etc.), often featuring almost unlimited resources, but also by skilled individuals due to the accessibility of the attacks source code. In this alarming scenario, the selection of the optimal set of countermeasures to fire against those attacks represents a primary necessity. While significant effort has been made toward the standardization of the representation of security-related knowledge such as vulnerabilities, weaknesses, and attacks, the intelligence surrounding the countermeasures field received considerably less attention. The paper at hand aims at contributing to the reaction ecosystem by proposing a standard representation of the countermeasure instances. With such a proposition, we address one of the critical challenges found in the literature, that is, the absence of a commonly-shared definition of remediations. To demonstrate the feasibility of our approach, we present several scenarios where some relevant countermeasures are efficiently enforced, resulting in mitigating the ongoing cyberthreat. Then, the advantages and disadvantages of our proposal are extensively discussed, opening the debate for novel and effective contributions in this research line.

Keywords

Countermeasure selection · Cyberattack countermeasures · Countermeasure standardization · Intrusion reaction systems · Reaction intelligence sharing.

3

AIS-powered Optimal Countermeasures Selection

Title:	A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection
Authors:	Pantaleone Nespoli, Félix Gómez Mármol, Jorge Maestre Vidal
Journal:	IEEE Access
JIF:	3.745 Q1 (2019)
Publisher:	IEEE
Volume:	9
Pages:	60971–60996
Year:	2021
Month:	Apr
DOI:	10.1109/ACCESS.2021.3074021
Status:	Published

Abstract

Nowadays, Information and Communication Technology (ICT) infrastructures play a crucial role for human beings, providing essential services at astonishing speed. Nevertheless, such a centrality of those infrastructures attracts the interest of ill-motivated actors that target such infrastructures with cyberattacks that are every day more sophisticated and more disruptive. In this alarming context, selecting the optimal set of countermeasures represents a primary need to react against the appearance of potentially dangerous threats effectively. With the motivation to contribute to developing faster and more effective response capabilities against them, the paper at hand introduces a novel cybersecurity reaction methodology based on Artificial Immune Systems (AIS), for which the evolutionary computing paradigm has been adopted. By leveraging the outstanding properties of these bio-inspired techniques, the selected countermeasures to defeat cyberthreats through cloning and mutation phases in an effort to improve the quality of the solution from a quantitative perspective, being able to adjust the risk to which the assets of the protected system are exposed. Exhaustive experiments demonstrate the feasibility of the proposed approach, reducing the risk in a more than acceptable time lapse.

Keywords

Countermeasure selection · Cyberattack countermeasures · Intrusion reaction systems · Artificial immune systems · Bio-inspired reaction.