International Journal of Information Security (2025) 24:122
https://doi.org/10.1007/s10207-025-00985-6

REGULAR CONTRIBUTION

SERDUX-MARCIM: Maritime Cyberattack simulation using Dynamic Modeling, Compartmental Models in Epidemiology and Agent-based Modeling

Diego Cabuya-Padilla[1] · Daniel Díaz-López[2] · Juan Martínez-Páez[3] · Laura Hernández[3] · Carlos Castaneda-Marroquin[2]

Abstract
Cybersecurity protects computer data, programs, systems, and networks from unauthorized access, attacks, or theft. By studying cyberattacks, cybersecurity professionals gain insights into attackers' tactics, techniques, and methods, which are crucial for developing effective defense strategies and preventing future attacks. This paper introduces SERDUX-MARCIM, a model for simulation, modeling, and analyzing cyberattacks' propagation in maritime infrastructure, considering network-specific characteristics and target and attacker capabilities. This proposal is supported by a simulation environment in Matlab and Netlogo, considering some of the most accepted cyber risk assessment methodologies and compartmental models in epidemiology. Considering the complexities of the maritime sector. SERDUX-MARCIM is also validated through extensive experimentation in different attack scenarios that represent real-world cyber campaigns in the maritime sector, showing the effectiveness of our proposal.

Keywords Agent-based modeling · Compartmental models · Cyberattack · Cyberdefense · Cybersecurity · Cyber risk · Cyber threats · Dynamic modeling · Maritime cybersecurity · Naval · Cyber situational awareness.

1 Introduction

The computer systems, networks, programs, and data essential for the vital functioning of a society, which are known as critical infrastructures, are increasingly exposed to different dangers in cyberspace [1]. Critical infrastructures are present in sectors such as energy, transport, finance, telecommunications, water supply, and government services, among others, which may generate severe social impacts during an attack. Other sectors with critical infrastructure are healthcare and maritime [2]. Under this situation, cybersecurity offers countermeasures aimed at detecting, preventing, and mitigating risks in such cyberspace, supporting the resilience and reliability of critical infrastructures, and avoiding the potential impact of the materialization of such risks, which could endanger public safety, national security, and economic stability [3]. A cyberattack may take various forms, such as malicious code or malware, cross-site scripting, injection, or social engineering, and poses a significant risk to critical infrastructure [4]. Thus, understanding the patterns and trends related to threats in critical infrastructures is essential; however, designing and developing appropriate cybersecurity countermeasures is also important.

Cyber Situational Awareness (SA) is defined as "a three-phase process that allows security analysts to perceive (sense) the status of an enterprise network, comprehend the current situation, and make predictions based on the

✉ Daniel Díaz-López
danielo.diaz@urosario.edu.co

Diego Cabuya-Padilla
diego.cabuya@enap.edu.co

Juan Martínez-Páez
juandi.martinez@urosario.edu.co

Laura Hernández
laurava.hernandez@urosario.edu.co

Carlos Castaneda-Marroquin
ccastaneda@servalnetworks.com

1 Engineering Faculty, Naval School "Admiral Padilla", Tv 52 # 17-150 Isla Manzanillo, Cartagena 130001, Colombia

2 School of Engineering, Science, and Technology, Universidad del Rosario, Carrera 6 # 12 C - 16, Bogotá 111711, Colombia

3 Serval Networks, Av. de la Industria, 4, Alcobendas, Madrid 28108, Spain

Published online: 02 May 2025

knowledge acquired" [5]. This process is critical for ensuring informed decision-making across strategic, tactical, and operational levels, particularly as cyberattacks become increasingly sophisticated and impactful. Within this framework, the SERDUX-MARCIM model contributes to the strategic dimension of CSA by equipping naval executive officers with a high-level tool to guide decisions during cyberattacks on maritime infrastructure. Its design abstracts from specific protocols and technologies, enhancing its adaptability and versatility across diverse maritime scenarios.

Cybersecurity researchers and professionals can gain insights into malicious actors tactics, techniques, and procedures (TTPs) by studying cyberattacks. Understanding such TTPs is essential for developing effective defense strategies and mitigating future cyberattacks. A cyberattack has the following attributes [6]: i) attack vector, which is the route to gain access to the target; ii) payload, which refers to a component designed to perform a specific harmful action on the target, iii) exploit, which is the code that exploits a vulnerability in the target to implant a payload, and iv) vulnerability, which is a technical failure or a deficiency existing in the target. Some cyberattacks spread with behavior similar to biological viruses, suggesting that compartmental models in epidemiology can be used to understand how such cyberattacks spread and their effects, identical to the spread of an infectious disease in an individual or population [7].

There are various compartmental models [8], with the SIR model being one of the most well-known. In the SIR model, individuals in a population are classified into three compartments: *Susceptible* (S), *Infectious* (I), and *Recovered* (R). The susceptible compartment includes individuals who become infected upon contact with contagious individuals. Individuals in the susceptible or infectious compartment may eventually go to the recovered compartment if they receive a treatment, e.g., a vaccine. The SEIR model extends the SIR model by introducing an additional compartment for *Exposed* (E) individuals, which represents individuals who have been exposed to the disease but are not yet showing symptoms of infection. After a latent period, during which the infection evolves inside the individual, individuals in the exposed compartment may move to the infectious compartment. Applying these epidemiological models in a cybersecurity environment allows researchers to gain a deeper understanding of the proliferation of cyber threats and design robust defense mechanisms in an anticipated way [9].

Cybersecurity risk management is a crucial concern in the maritime sector because it is generally composed of a complex network with multiple stakeholders, such as maritime authorities, shipping companies, the navy, coast guard, shipping ports, and logistic operators, who increasingly rely on digital systems for communication, location, and transit, among others [10, 11]. More than 80% of world merchandise trade by volume is carried by sea [12], and it depends on sensitive information, such as cargo details, port schedules, port operations, and financial data; thus, protecting this information is of utmost importance. Cyberattacks in the maritime sector can disrupt operations, putting the safety of crew and cargo at risk, damaging a company's reputation, generating legal controversies, causing financial losses [11], and even geopolitical incidents between nations. Digital transformation has boosted the maritime sector in recent years; however, it has also implied the integration of Information Technologies (IT) and Operational Technologies (OT) devices with legacy technologies [13], which were not originally designed to be connected to the internet, exposing vulnerabilities that a threat agent can exploit [10].

For the case of maritime cybersecurity, the systematic review presented by Martínez et al. [7] identified various documents related to cybersecurity in the maritime sector produced by both public and private entities. However, most identified frameworks focus on establishing a foundational structure for managing cybersecurity. This review revealed a lack of consistency regarding the objectives, methodologies, and approaches. Additionally, the comparisons presented indicate that industry standards largely influence the characterization of methodologies, models, and frameworks. Despite the emergence of several processes aimed at integrating these practices into the maritime domain, significant work is required to ensure that cybersecurity management tools can be fully applied to the unique challenges faced in naval settings.

Addtionally, the bibliometric studies and document analysis presented by Cabuya-Padilla and Castaneda-Marroquin [14] concluded that maritime cybersecurity and cyberdefense research has predominantly focused on ships, thereby lacking a holistic perspective on the maritime system's complexity. A significant gap in the literature and low scientific output indicate opportunities for research on holistic approaches and modeling methodologies. The involvement of multiple stakeholders necessitates systems thinking and data science methods, such as agent-based modeling. Modern models often incorporate time-dependent rates to capture the evolving nature of cyberattack scenarios. Analyzing cyberattacks through "Network" and "Node" approaches provides a comprehensive understanding, with the former examining interactions among all nodes and the latter optimizing individual components. However, few models specifically address cyberattacks in the maritime sector, and existing models lack time-dependent rates and primarily focus on defensive perspectives.

Maritime cybersecurity regulations aim to enhance the resilience of maritime infrastructure, vessels, and port facilities against cyber threats, ultimately ensuring the safety, security, and reliability of maritime operations in an increasingly digitized environment [15, 16]. Maritime cybersecurity regulations have been implemented to maintain the pace

of increasing cybersecurity threats to the maritime industry. Thus, the International Maritime Organization (IMO) recognized the importance of cybersecurity in the maritime sector [17] and introduced in 2017 the Maritime Cyber Risk Management in Safety Management Systems through Resolution MSC.428(98) [18], later updated in 2022 with the document Guidelines on Maritime Cyber Risk Management [19], which provide recommendations for safeguarding ships and port facilities against cyber risks. Such guidelines, which are based on widely recognized principles, frameworks, standards and best practices, such as Information Security Management System (ISO) 27001 [20] and National Institute of Standards and Technology (NIST) Cybersecurity Framework [21], do not define mandatory elements to be fulfilled; instead, they are optional elements that a maritime company can follow. In addition, some other guidances can orientate maritime cyber risk management such i) Guidelines on cybersecurity on board Ships issued by Baltic and International Maritime Council (BIMCO) [22], ii) International Association of Classification Societies (IACS) Recommendation on cyber resilience [23], and iii) International Association of Ports and Harbors (IAPH) Cybersecurity Guidelines for Ports and Port Facilities [24].

Management systems that consider a cybersecurity perspective and include cyber risks are increasingly being adopted by the maritime industry; thus, maritime operations must adopt risk models with a cybersecurity baseline [13]. This step increases resilience against cyber threats, safeguard critical assets and infrastructure, and ensures the maritime sector's safe and secure functioning.

Under the previous context, this paper proposes SERDUX-MARCIM, a maritime infrastructure protection model that allows the analysis of cyberattacks through compartmental epidemiology models that align with widely recognized cyber risk assessment methodologies. Such a model represents a fresh adaptation of compartmental models in epidemiology, like SIR or SEIR, into a context of dissemination of cyberattacks in maritime contexts, considering the characteristics of the cyberattack and the propagation dynamic. Additionally, the SERDUX-MARCIM model incorporates updates and introduces new time-dependent transition rates, which include network-specific attributes, target/attacker capabilities, and cyberattack characteristics, thus enabling simulations that closely mirror the complexities of real-world cyberattacks. The primary contributions of this paper are:

1. The proposal of the SERDUX-MARCIM model to analyze and forecast the propagation of a cyberattack over a maritime infrastructure, considering, the cyberattack and network-specific characteristics and target and attacker capabilities.
2. The cyber risk assessment methodology proposal to determine the likelihood and can help in making informed risk management decisions considering technical and business issues.
3. The stability analysis for each parameter is included in the SERDUX-MARCIM model to validate the behavior obtained according to the parameter's values change.
4. The development of a simulation environment in Matlab and NetLogo that allows experimentation with the SERDUX-MARCIM model at the network and node levels.
5. The validation of the SERDUX-MARCIM model in a real-world case based on the attack on Maersk in 2017 by the ransomware NotPetya.

This paper is organized as follows. Section 2 introduces the core elements required to construct SERDUX-MARCIM proposal. Section 3 reviews researches that analyze cyberattack propagation at node and network levels using epidemiological models. Section 4 defines the SERDUX-MARCIM model according to the states of nodes and dynamics provided by compartmental epidemiological models and introduces the cyber risk assessment methodology proposal for the maritime sector. Section 5 establishes the Cyber Risk Approach to calculate the risk, likelihood, and impact value of a cyberattack in the maritime sector during the simulation development using SERDUX-MARCIM. Section 6 defines the System of Differential Equations in SERDUX-MARCIM, including the formulation of the time-dependent transition rates in it, which consider the actions taken by the target to prepare for and counter the cyberattack generated by the attacker, which influences the outcome over time. Section 7 presents the experimental results of executing the SERDUX-MARCIM model in a real-world cyberattack scenario. Section 8, which is the validation of the SERDUX-MARCIM model through its application in a real-world cyberattack case that occurred in 2017 to the maritime company Maersk using the ransomware NotPetya. Finally, Sect. 9 presents the primary outcomes of this research and highlights future research.

2 Background

2.1 MARCIM

MARCIM is the Framework for Modeling and Simulation of Maritime Cyberdefense (MARCIM) addressed to strategic level scenarios [14], which defines maritime entities, actions executed by entities, and types of interactions between entities. This framework allows experimenters to develop/test working hypotheses or courses of action, understand the complexity of the maritime technological ecosystem, and determine possible attack and defense scenarios. The MARCIM framework outlines a group or individuals

involved in maritime cybersecurity and cyberdefense, known as *Maritime Cyberdefense Key Actors*, which take actions and interact with other actors and components in the system. A specific set of cyber capabilities can also identify individual actors. In brief, the MARCIM defines four types of Maritime Cyberdefense Key Actors, which are described below. Examples of actors of each type can be found in Table 1 [25].

- Maritime: An individual, group, or entity that plays a significant role in the maritime domain, whether by providing maritime services, providing services to the maritime sector, or contributing to maritime management and development.
- Cyber Threat: An individual or group that intentionally causes harm or negative effects on devices, systems, or networks can be categorized based on motivations, skill level, and tactics.
- Security and Defense: A group or entity that protects a nation's digital infrastructure and information systems from cyber threats. It can support and assist maritime actors during cyberattacks.
- Coordination and Cooperation: An entity or organization responsible for coordinating and collaborating on cybersecurity initiatives at the national level. These actors create plans, systems, and alliances to share information and improve the country's cybersecurity.

MARCIM defines the *Cyber-Kinetic Reference Model* [25], shown in Fig. 1, which is a conceptual approach that integrates maritime cybersecurity and cyberdefense actors to provide a clear understanding of the main interactions and effects. It helps create effective defense strategies and capabilities by analyzing the interplay between the operational cyber capabilities of actors. The model considers two main groups: i) the *Blue Team*, which includes Maritime (Target), Security and Defense (Defender), or Coordination & Cooperation (Support the Defender or Target) actors, who are responsible for protecting systems, networks, and data from unauthorized access, breaches, and attacks, and ii) the *Red Team*, which includes Cyber Threat (Attacker) and Coordination & Cooperation (Support the Attacker) actors, which play an offensive role in identifying and exploiting vulnerabilities to create a negative effect on the Blue Team. In such a model, the first line of defense is in charge of the Maritime actor, and the second line of defense includes the Security and Defense actor. Additionally, the relation between the actors of this "Cyber-Kinetic Reference Model" is defined by the arrows that connect them, which can be offensive, defensive, or collaborative.

Finally, MARCIM also defines the *Cyberdefense Capabilities Model*, which encompasses a broad range of resources, assets, tactics, techniques, processes, procedures, and skills that enable actors to secure and defend cyber assets and perform effective cyber operations. These capabilities include both "Operational" and "Support and Sustainability" capabilities.

Table 1 MARCIM type of actors and examples

Type	Examples of actors
Maritime	Maritime authorities
	Port terminals and operators
	Ships, cargo, and facilities
	Maritime industry
	Maritime information and communications
	service providers
	Maritime transportation system operators
	Maritime management service providers
	Suppliers and intermodal partners
Cyber threat	Nation-States
	Foreign intelligence services
	Cybercriminals
	Industrial spies
	Hacktivists
	Terrorist groups
	Insider threats
	Thrill-seekers
	Illegal organizations
	Individuals
	Advanced persistent threats
Security and defense	Military forces
	Navy force
	Naval cyber unit
	Cyber joint command
	National police
	Cyber police center
	National CERT / CSIRT
Coordination and cooperation	National Government Institutions
	International agencies, Organizations or Institutions
	Academy
	Private sector
	Trade unions and professional associations
	Others non-formal

2.2 Cyber risk concepts

Some key concepts regarding cyber risk management are introduced next, primarily the OWASP Risk Rating Methodology, D5 effects, and the security control categories, which are fundamental to understanding the proposal to be developed in the following sections.

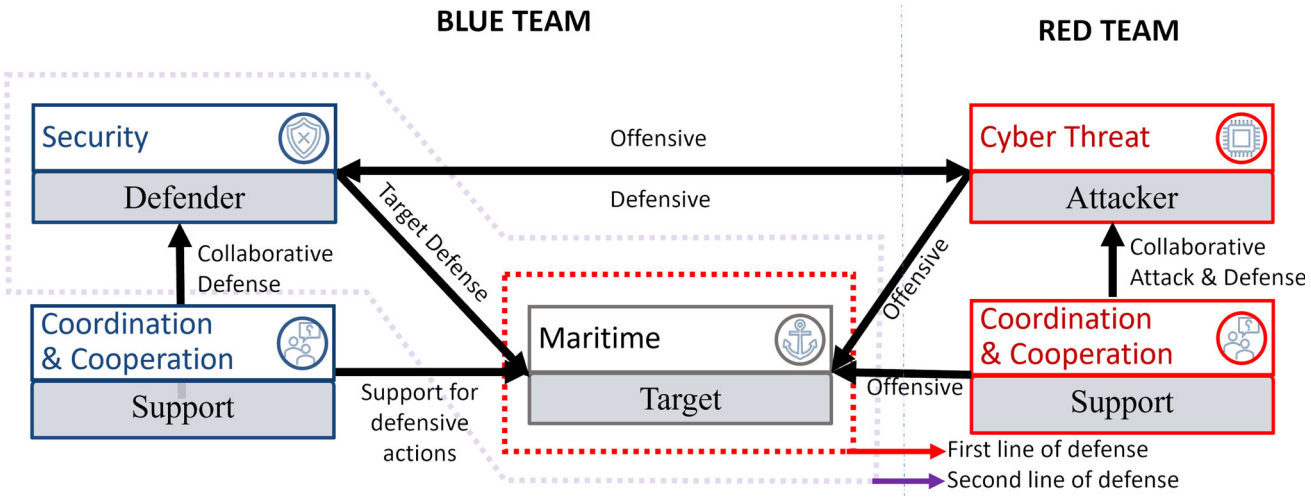


Fig. 1 Cyber-Kinetic reference model for maritime cyberdefense (Adapted from [25])

A risk methodology that is a reference in the industry is the *Open Worldwide Application Security Project (OWASP) Risk Rating Methodology* [26], which is a structured approach for evaluating and managing security risks associated with a business. The model consists of six steps: identifying risks, estimating the likelihood of occurrence, estimating the impact of the risk, determining the severity, deciding which risks to address, and customizing the risk rating model. This methodology is based on classic risk theory, which asserts that risk is the product of the likelihood of an event and its impact. This methodology helps testers gather information about threats, assess the likelihood and impact of security risks, and determine the overall severity of a risk.

The OWASP Risk Rating Methodology calculates likelihood and impact by considering a set of factors and sub-factors, as shown in Table 2, and has a unique approach that considers factors related to the attacker and victim. The sub-factors associated with the attacker, i.e., the threat agent, allow characterization of the attacker's offensive capacities and motivations. The subfactors related to the victim, i.e., vulnerability, technical, and business impact, allow identification of the victim's exposure to an attack. All these factors allow us to determine risk severity from a holistic perspective.

Determining the impact of a cyberattack is important for differentiating offensive campaigns and profiling the threat agent. An interesting way to evaluate this impact was proposed by Jabbour and Poisson [27] using the five D5 effects: Disrupt, Deny, Degrade, Destroy, and Deceive. These effects represent the impact of a cyberattack in terms of severity and duration. MITRE Corporation adopts the D5 effects in the document "Assessment of Operational Energy System Cybersecurity Vulnerabilities" [28], which presents a methodology to assess cybersecurity risks in distributed information systems, which may help organizations determine their preparedness against cyber threats. The D5 effects are represented in Fig. 2 and are defined next:

Table 2 OWASP risk rating methodology factors and sub-factors

Risk	Factor	Sub-factor
Likelihood	Threat agent	Skill level
		Motive
		Opportunity
		Size
	Vulnerability	ease of discovery
		Ease of exploit
		Awareness
		Intrusion detection
Impact	Technical impact	Loss of confidentiality
		Loss of integrity
		Loss of availability
		Loss of accountability
	Business impact	Financial damage
		Reputation damage
		Non-compliance
		Privacy violation

1. Disrupted (Delay): A break or interruption occurs in the flow of information or functionality with a temporary duration. The effect intended by the attacker is achieved but not within the intended time.
2. Degraded: A partial reduction in the cyber asset's effectiveness or efficiency, either permanent or extensive duration. The attacker achieves some, but not all, of the intended effects or achieves all intended effects only after taking additional actions.
3. Denied: There is a total prevention in the access and use of a cyber asset with a temporary duration. The attacker

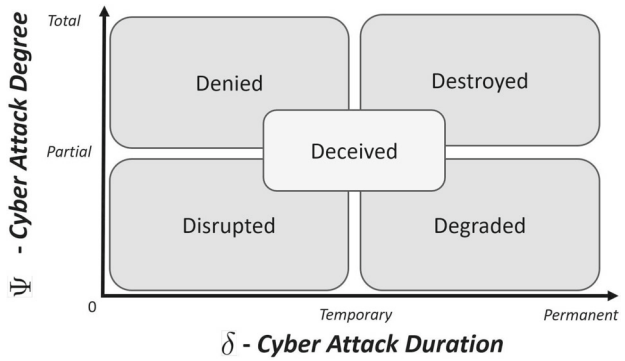


Fig. 2 D5 effects (Adapted from [27])

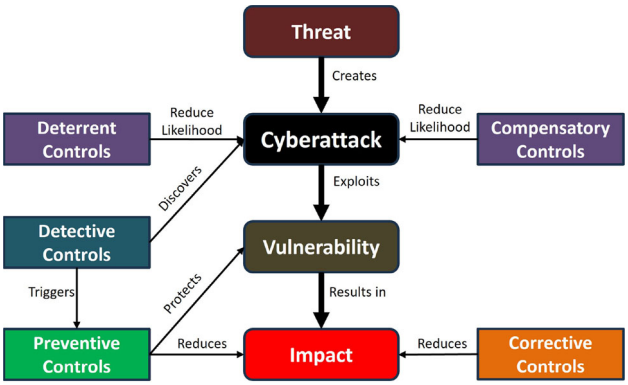


Fig. 3 Relation between security controls and risk according to ISACA

attempts to make a cyber asset totally unavailable to its intended users.

4. Destroyed: A cyber asset is damaged so badly that it cannot perform a function or be restored to a usable condition without being completely rebuilt.
5. Deceived: To cause a target to believe what is untrue, to mislead the target's decision-makers by manipulating their perception of reality. Deceive effect can have a temporary or permanent duration and a partial or total degree. This effect is represented at the center of Fig. 2 because it can achieve any of the other four effects.

Security controls or countermeasures are critical to asset protection and are generally categorized according to their function. A well-accepted security control categorization was proposed by Information Systems Audit and Control Association (ISACA), which defines the 5 categories listed in Table 3 [29, 30]. Security controls play a role before, during, or after the execution of an attack or the occurrence of a security violation, depending on the category to which they belong. Specifically, security controls directly decrease the risk components, reducing the likelihood or impact of a cyberattack, as shown in Fig. 3 [29]. Generally, combining security controls from different categories is the best strategy to handle cybersecurity risks.

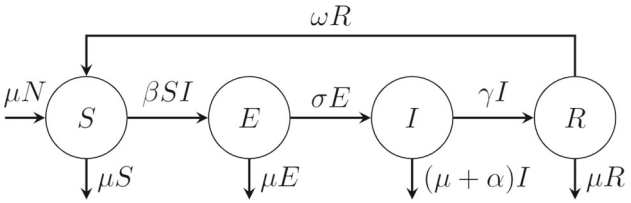


Fig. 4 SEIR model flow diagram [7]

2.3 Epidemiological model in cybersecurity

Epidemiological compartmental models in cybersecurity have evolved substantially in the last few years. Initially, models such as SIR [31] were used to understand the spread of computer viruses and malware, focusing primarily on susceptibility, infection, and recovery aspects. As cyber threats become more complex, new models like SEIR [32] and SEIRS [33] emerged, which include the latency period before an exposed node becomes infectious, providing, in such a way, a more comprehensive understanding of the dynamics of cyber infections. In recent years, advanced frameworks like MalSEIRS [7] have been proposed to analyze malware spread considering the unique characteristics of cyber threats, such as potential re-infection and the impact of security countermeasures on malware spread. SEIRS and MalSEIRS models are explained next.

2.3.1 SEIRS model

The SEIRS model divides the population into four states: *Susceptible* (S), *Infected* (I), *Recovered* (R), and *Exposed* (E) [33]. Each individual belongs to a single state at a time. The model assumes a static population with no death rate, meaning that the *Total Population Size* (N) remains constant throughout the pandemic, as indicated in Eq. 1.

$$N = S + E + I + R \tag{1}$$

The SEIRS model allows the following transitions between states:

- ($S \rightarrow E$): A node when a payload is installed on the node, but the payload has not been executed on the node.
- ($E \rightarrow I$): A node becomes infected when it has infection symptoms due to the execution of a payload.
- ($S \rightarrow R$): A node recovers when security measures are applied over it, making it immune to the infection.
- ($R \rightarrow S$): A node becomes vulnerable when it does not have a security measure that helps it resist infection or the immunity gained by the node is lost, thereby making it susceptible to reinfection.

Table 3 Security controls categorization according to ISACA

Control	Description
Preventive	Inhibit security policy violations
Detective	Warn about violations or attempted violations of the security policy
Corrective	Remedy the impact of a violation
Compensatory	Reduce the risk that a weakness in an existing control can be exploited
Deterrent	Generate warnings that prevent potential violations

Table 4 Rates for the SEIRS model [7]

Parameter	Definition
β	Malware propagation rate
γ	Malware removal rate
σ	Malware execution rate
ω	Rate of loss of antiviruses and security measures (loss of immunity rate)
α	Machine unavailability rate caused by malware
μ	Machine unavailability rate caused by other reasons

The SEIRS model in Fig. 4 has susceptible nodes that become exposed at a rate $\beta \in [0, 1]$, and becoming recovered at a recovery rate $\gamma \in [0, 1]$. The exposed population is infected at a rate $\sigma \in [0, 1]$. Nodes may lose immunity before infection and recovery at a rate $\omega \in [0, 1]$. A machine unavailability rate is caused by other reasons different to the cyberattack $\mu \in [0, 1]\mu \in [0, 1]$. Infected nodes may also become unavailable by the malware at rate $\alpha \in [0, 1]$. Finally, new nodes"births" at a rate μN. Table 4 contains a summary of the rates of the SEIRS model.

Finally, Eq. 2, taken from [33], shows the system of equations that define the total population size in each state over time.

$$\begin{cases} \frac{dS}{dt} = \mu N - \frac{\beta I S}{N} + \omega R - \mu S, \\ \frac{dE}{dt} = \frac{\beta I S}{N} - \sigma E - \mu E, \\ \frac{dI}{dt} = \sigma E - \gamma I - (\mu + \alpha) I, \\ \frac{dR}{dt} = \gamma I - \omega R - \mu R \end{cases} \tag{2}$$

The system of differential equations in Eq. 2 mathematically represents the dynamics of malware within a population of nodes using the SEIRS framework, which was established by Bjørnstad et al. [33]. The evolution of the number of nodes in each state–Susceptible (S), Exposed (E), Infected (I), and Recovered (R)–is governed by a set of coupled first-order differential equations. The rate of change in the susceptible population is influenced by the addition of new nodes (μN) and the reduction of immunity due to the loss of security measures (ωR). Susceptible nodes are lost due to malware infections ($\beta I S$) or machine unavailability caused by other reasons (μS). The exposed population increases as susceptible nodes become infected and progress to the infected state (σE), whereas losses occur due to machine unavailability caused by other factors (μE). The infected population grows as exposed nodes become infected but decreases due to malware removal (γI) or machine unavailability caused by malware or other factors ($(\mu + \alpha) I$). Finally, the recovered population increases as infected nodes recover; however, it decreases over time due to the loss of immunity (ωR) and machine unavailability caused by other factors (μR). The proposed system captures both malware transmission dynamics and machine failures due to other causes, providing a comprehensive mathematical description of network states and transitions over time.

2.3.2 MalSEIRS

The MalSEIRS malware propagation model [7] characterized by Eq. 3, taken from [7], is a modification of the SEIRS model to allow: i) adaptation of infection, recovery, and loss of immunity rates to make them time-dependent, ii) inclusion of births in the context of computer networks, and iii) addition of the concept of a vaccine to shield recovered nodes.

$$\begin{cases} \frac{dS}{dt} = p\Lambda - \beta(t) I S + \omega(t) R - (\mu + \phi) S, \\ \frac{dE}{dt} = \beta(t) I S - \sigma E - \mu E, \\ \frac{dI}{dt} = \sigma E - \gamma(t) I - (\mu + \alpha) I, \\ \frac{dR}{dt} = (1 - p)\Lambda + \gamma(t) I - \omega(t) R - \mu R + \phi S. \end{cases} \tag{3}$$

Where $\beta(t), \gamma(t), \omega(t) \in [0, 1]$ denote the *Malware Propagation Rate*, *Recovery Rate*, and *Loss of Immunity Rate*. In addition, $\phi, p \in [0, 1]$, $\Lambda \geq 0$ denote the *Immunization Rate*, *Birth Susceptibility Rate*, and *New Node*s that connect to the network. Finally, $\mu, \sigma, \alpha \in [0, 1]$ denote the *Machine Unavailability Rate Caused by Other Causes*, the *Malware Execution Rate*, and the *Machine Unavailability Rate Caused by Malware*, correspondingly.

The MalSEIRS malware propagation model [7], described by Eq. 3, modifies the SEIRS framework to incorporate: (i) time-dependent infection ($\beta(t)$), recovery ($\gamma(t)$), and loss

of immunity rates ($\omega(t)$); (ii) the inclusion of new nodes entering the network, modeled by a birth susceptibility rate ($p\Lambda$); and (iii) an immunization mechanism where recovered nodes can regain protection (ϕS).

The system of differential equations defines the number of nodes in each state–Susceptible (S), Exposed (E), Infected (I), and Recovered (R)–and their transitions. The susceptible population changes due to node entries ($p\Lambda$), infections from infected nodes ($-\beta(t)IS$), and loss of immunity from recovered nodes ($\omega(t)R$), with losses due to machine unavailability and other causes ($-(\mu+\phi)S$). Exposed nodes increase through infections and decrease due to progression to the infected state (σE) and unavailability (μE). The infected population grows as exposed nodes become infectious but declines through recovery ($\gamma(t)I$) and machine unavailability ($(\mu+\alpha)I$). Lastly, the recovered population is affected by recovered nodes ($\gamma(t)I$), loss of immunity ($\omega(t)R$), and the immunization mechanism (ϕS). This model captures malware dynamics and network-wide adaptive responses over time.

3 State of the art

Cybersecurity and cyberdefense are significant concerns for all critical infrastructures, as most rely on interconnected technologies to improve efficiency, operational capabilities, and secure functioning against evolving cyber threats. Recent research has investigated cyberattack propagation behavior at both node and network levels, focusing on epidemiological and agent-based models. This section presents the most notable studies related to this research object.

Kotenko [34] presented an approach to simulate cyberwars, focused on Distributed Denial of Service (DDoS) attacks and associated countermeasures. This approach employs agent-based modeling to represent cyberwarfare as a collection of semi-autonomous agents interacting with each other. The conclusions presented in this paper demonstrate the need for an integrated adaptive security system that can operate in adversarial environments to protect large-scale systems.

Kotenko [35] later developed a multi-agent simulation framework for investigating distributed cooperative multilevel cyberdefense, which helps simulate cyberattacks and cyber protection mechanisms through agent-based simulation. Two experiments were conducted on adapting the attack and defense teams and the cooperation modes between the defense teams. The defense methods used were: Hop Counts Filtering (HCF), Bit Per Second (BPS), and Source IP address Monitoring (SIPM). This study concluded that team cooperation leads to an effective defense, which should consider aspects like the network topology and configuration, the structure and configuration of attack and defense teams, the attack and defense mechanisms, and the cooperation between the defense teams.

Dobson and Carley [36] introduced the "Cyber-Forces Interactions Terrain (Cyber-FIT)" simulation framework. This allows the development of experiments around cyberwarfare in different terrains and against various adversarial forces. This framework defines two classes of agents, namely forces and terrains. Forces can be defensive or offensive depending on whether they protect or attack the assigned cyber terrain. In contrast, terrain refers to the computer systems that military units rely on to execute their missions. It can be of three types: networking, server, and user systems. The outputs of this innovative simulation framework were represented primarily in the time-dependent variables: vulnerability rate per terrain type, compromise rate per terrain type, and overall mission capability rate.

Hernández et al. [37] presented "SCIRAS: Model for Advanced Malware Propagation", which is a mathematical model to simulate the offensive behavior of advanced malware, e.g., Advanced Persistent Threat (APT), which exploits zero-day vulnerabilities. This paper discusses an advanced malware model that can identify potential targets and determine whether to attack them. Such model are compartmental, deterministic, and global, and their dynamics are based on a System of Ordinary Differential Equations (SODE), which define 5 states for a device: susceptible, carrier, infected, attacked, and recovered. Finally, some recommendations are proposed that can help define security countermeasures against APTs and understand the dynamics of advanced malware propagation.

Later, Martínez et al. [7] proposed a model named Mal-SEIRS, inspired by the SEIRS epidemiological model, to predict malware propagation in a network. This model considers time-dependent rates, such as infection, recovery, and loss-of-immunity rates, which allows modeling dynamic scenarios where conditions change during a cyberattack. In addition, it presents exhaustive experiments to help develop defensive and offensive strategies that can be incorporated into a playbook for Computer Security Incident Response Teams (CSIRT).

Kavallieratos et al. [38] introduced a method for analyzing the propagation and aggregation of risks in complex Cyber-Physical Systems (CPSs). This is applied in navigational systems of Cyber-Enabled Ship (C-ES) from 2 types: i) Autonomous ships equipped with advanced interconnected CPSs able to navigate without human intervention, and 2) Remotely controlled ships equipped with CPSs that allow control and operation from the shore. Five threats applicable to maritime components were analyzed: spoofing, tampering, repudiation, information disclosure, and denial of service. For each threat, the model proposed a set of 20 cybersecurity controls that minimize the residual risk and implementation cost, e.g., in autonomous ships, spoofing attacks can be

addressed using the following controls: generate time stamps, inspect unsuccessful login attempts, restrict remote access, and security assessments.

Moreover, Francia et al. [39] proposes an Agent-based Model (ABM) to predict entities' behavior in cyberspace and establish a foundation that helps in decision-making processes related to cybersecurity resource allocation, strategic planning, and policy enforcement. This model is based on the Susceptible-Infectious-Susceptible (SIS) model used in epidemiology, and the simulations obtained from this model were based on the continuous-time Markovian SIS model. The model was tested in different scenarios, for which the infection and recovery rates were studied over time, considering the various levels of sophistication of the adversary side.

Finally, Sepúlveda [40] proposed an epidemiology-based approach to modeling the structure of a system that is conditioned to an infection and an eventual recovery due to zero-day malware cyberattacks. This approach considers the system's structure and flows to represent causal connections between strategic-level variables that simulate many aspects of an IT system, like the functional features, vulnerabilities, and programmers. This study also proposes recommendations for resilience building and security policies to combat cyber threats. It emphasizes treating cyber threats as a public health issue rather than just a competitive factor.

The previous studies have demonstrated progress in modeling cyberattack propagation at individual and system levels. Thus, a comparison of these related works in terms of some key factors is presented in Table 5.

Overall, there is a growing trend of using Agent-based Modeling and other techniques, such as Dynamic Modeling and Evolutionary Programming, to tackle the intricacy and dynamism of computer networks and cyberattacks. Another significant approach in this regard is using Compartmental Models in epidemiology. Our proposal SERDUX-MARCIM is remarkable because it obtains the best from three different techniques, i.e. Dynamic Modeling, Compartmental Models in epidemiology, and Agent-based Modeling, to compose a solution that adapts a well-known compartmental model, can offer an agent perspective as part of a large dynamic system that changes as a cyberattack advances.

Due to the nature and complexity of cyberattacks, more modern models incorporate time-dependent rates to represent the changing nature of a cyberattack scenario. The number of time-dependent rates and their definition depends on their purpose in the model, as some represent the attacker or target behavior during a cyberattack campaign. Our proposal, SERDUX-MARCIM, uses five time-dependent rates to model the complex dynamism of a cyberattack addressed against a maritime infrastructure.

Most related works propose models from a defensive perspective, however, SERDUX-MARCIM examines cyberattacks from offensive and defensive perspectives to generate more accurate outcomes and provide additional information beyond the defensive viewpoint.

Analyzing a scenario from *Node* and *Network* approaches allows to understand a cyberattack holistically. On the one hand, the *Network* approach allows a comprehensive examination of all network's nodes, identifying interactions between them. This approach helps predict network behavior under various conditions and scenarios, which is critical for decision-making. In contrast, the *Node* approach enables a detailed examination of individual components that contribute to each node's optimization, gaining local efficiency and contributing to the Network's overall performance. In this sense, SERDUX-MARCIM integrates Node and Network approaches, allowing a general and specific analysis of cyberattack.

As far as we know, there are not many models that tackle the problem of modeling cyberattacks for the maritime sector, and the only one identified does not include time-depend rates and considers only a Defensive perspective and a Network approach [38]. The SERDUX-MARCIM model proposed in the paper is specifically designed to model cybersecurity attacks in the maritime domain and employs multiple approaches, including analysis of cyber risks, cyber warfare, and cyberattacks. Finally, extensive experiments over SERDUX-MARCIM were executed and documented, and the source code is available to facilitate the reproduction of the results.

4 SERDUX-MARCIM proposal

This section describes the details of the proposed SERDUX-MARCIM model, which is an innovative way of integrating different concepts of a maritime domain in a cybersecurity landscape, with the aim of understanding the dynamic between attacker, target, and means of attack.

SERDUX-MARCIM model is a novel adaptation of compartmental epidemiological models applied to cybersecurity and cyberdefense. The proposed model is used to study the behavior and spread of cyberattacks, primarily in the maritime field. The proposed SERDUX-MARCIM model was named considering the integration between SERDUX and MARCIM. SERDUX represents an abbreviation of our proposal of the 6 states that a node can take at time t when a cyberattack is running: *Susceptible* (S), *Exposed* (E), *Resistant* (R), *Degraded* (D), *Unavailable* (U), and *Destroyed* (X). Additionally, MARCIM is a reference to the Framework for Modeling and Simulation of Maritime Cyberdefense (MARCIM) introduced at Sect. 2.1, from which some components are taken for the current proposal, such as the *Maritime Cyberdefense Key Actors*, the *Cyber-Kinetic Reference Model*, and the *Cyberdefense Capabilities Model*. These

Table 5 Legend: ✓ Yes – ✗ No. Comparison of related works

Table 5: Legend: ✓ Yes – ✗ No. Comparison of related works

Related Work	Related Modeling Type	Time Dependent Rates?	Perspective	Design Approach	Areas of Aplication	Code Availability?	Validation with Experiments?
Kotenko [34]	Agent-based Modeling	✗	Defensive and Offensive	Node and Network	Cyberattack Analysis, Cyberwarfare	✗	✓
Kotenko [35]	Agent-based Modeling	✓	Defensive and Offensive	Node and Network	Cyberattack Analysis, Cyberwarfare	✗	✓
Dobson et al. [36]	Agent-based Modeling	✓	Defensive and Offensive	Node and Network	Cyberwarfare	✗	✓
Hernández et al. [37]	Dynamic Modeling, Agent-based Modeling	✗	Defensive	Network	Cyberattack analysis	✗	✓
Martínez et al. [7]	Dynamic Modeling, Compartmental models in epidemiology	✓	Defensive and Offensive	Network	Cyberattack analysis,	✓	✓
Kavallieratos et al. [38]	Evolutionary Programming	✗	Defensive	Network	Maritime security, Cyber Risk	✓	✓
Francia III et al. [39]	Agent-based Modeling, Compartmental Models in epidemiology	✓	Defensive	Node and Network	Cyberattack analysis	✗	✓
Sepúlveda et al. [40]	Dynamic Modeling, Compartmental models in epidemiology	✓	Defensive	Network	Cyberattack analysis	✗	✓
Our proposal SERDUX-MARCIM	Dynamic Modeling, Compartmental models in epidemiology, Agent-based Modeling	✓	Defensive and Offensive	Node and Network	Maritime security, Cyber Risk analysis, Cyberattack analysis, Cyberwarfare	✓	✓

elements allow us to develop a model with a strategic focus on naval cyber operation. SERDUX-MARCIM holds the following features:

1. It enables network analysis and simulation of cyberattack propagation.
2. It integrates node states from compartmental epidemiological models, with the D5 Effects [27, 28].
3. It establishes a Cyber Risk Approach that considers known cyber risk assessment methodologies, such as OWASP Risk Rating Methodology [26], NIST Cybersecurity framework [21], ISACA Risk and information system control [29, 30], and IMO Guidelines on maritime cyber risk management [17].
4. It includes time-dependent transition rates that consider variations in network-specific characteristics, target capabilities, attacker capabilities, and cyberattack characteristics, thereby allowing a simulation that is closer to the complexity of a real system.
5. It is designed to study maritime domain cyber risks and cyberattack propagation at a network level considering its complexity.
6. It offers a simulation environment implemented in Matlab and NetLogo that allows practical simulations of cyberattacks at the network and node levels.

In this sense, the SERDUX-MARCIM model was designed with a strategic focus on naval cybersecurity and cyberdefense, addressing the maritime domain at a high level. CSA plays a critical role in enabling informed decision-making across strategic, tactical, and operational levels, and SERDUX-MARCIM contributes to the strategic dimension of CSA by equipping naval executive officers with a high-level framework to guide decisions during cyberattacks on naval infrastructure. Its primary application, as demonstrated in this study, pertains to shore facilities. However, the model is highly adaptable and can also be applied to vessels, which are conceptualized as systems of systems within the simulation framework. Each vessel system can be treated as a computational node, allowing the model to simulate complex interactions and disruptions across maritime networks. By generalizing key characteristics of maritime nodes, the model achieves a level of flexibility that facilitates its use across diverse scenarios and contexts, while maintaining its focus on strategic-level applications.

Additionally, SERDUX-MARCIM adopted some recognized cybersecurity definitions, frameworks, and methodologies from the cybersecurity field proposed by ISACA, MITRE, and OWASP which enrich our model. These approaches are not limited in applicability to one domain, but are quite general, robust and versatile, to allow their application in the maritime domain. By leveraging these best practices, our proposal aligns with established and effective frameworks from a broader cybersecurity landscape.

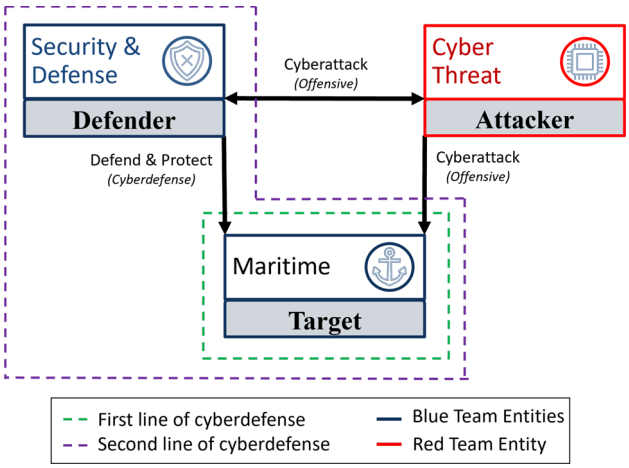


Fig. 5 Actors in SERDUX-MARCIM

4.1 Actors

Actors defined in the SERDUX-MARCIM model are depicted in Fig. 5, which is a simplified version of the *Cyber Kinetic Reference Model* explained in Sect. 2, which includes three types of maritime cyberdefense key actors: *Maritime*, *Security and Defense*, and *Cyber Threat*. *Coordination and Cooperation* was not considered between the actors of SERDUX-MARCIM, because it provides extra support in an ongoing cyberattack that would increase the target's cyberdefense capabilities; however, we are interested in modeling the behavior of the target with its capabilities.

The *Maritime* actor is a representation of an organization vulnerable to a cyberattack, i.e., a target that has a specific network configuration and holds certain *Cyber Capabilities* represented in *Operational Capabilities* and *Support and Sustainability Capabilities*. Examples of maritime actors include maritime authorities, port terminals and operators, ships and cargo facilities, maritime information and communications service providers, maritime transportation system operators, maritime management service providers, suppliers and intermodal partners, and national navies.

The *Maritime* actor's network N_{target} represents a set of connected cyber assets required for the target's operation. These are computational nodes with a hardware and software component, e.g., endpoints, routers, gateways, servers, Radio Detection and Ranging (RADAR), etc. Each of these cyber assets is a *Node* n_i, being every node an *Agent* in terms of agent-based modeling. Thus, a *Maritime* actor's network $N_{target} = \{n_1, ..., n_m\}$ is a set of m interconnected nodes in which a cyberattack may propagate.

The *Security and Defense* actor is the second line of cyberdefense of a *Maritime* actor against cyber threats and may contribute to improving its Cyber Operational Capabilities. Examples of security and defense actors include military forces, naval forces, naval cyber units, cyber joint commands, national police, cyber police centers, and national or sectorial CERTs/CSIRTs.

Activities that a *Security and Defense* actor may undertake include identifying security threats and risks, analyzing the network environment, and ensuring that the current state of security readiness is robust.

Finally, the *Cyber Threat* actor is an individual or group that intentionally causes harm or adverse effects, like the D5 effects introduced in Sect. 2.2, on the target's network by a cyberattack. The type of effect that a cyberattack can produce depends on the sub-factors associated with the attacker and the victim, which can be calculated according to the OWASP Risk Rating Methodology [26].

4.2 States

SERDUX-MARCIM model defines 6 states that a node can take at time t when a cyberattack is running: *Susceptible* (S), *Exposed* (E), *Resistant* (R), *Degraded* (D), *Unavailable* (U), and *Destroyed* (X). The definitions of these six states are given in Table 6.

In SERDUX-MARCIM, a *Cyberattack* is any action or attempt to cause damage to the *Maritime* actor's network. It is launched by a *Cyber Threat* actor using various strategies, such as malware, phishing, ransomware, and denial of service. It can affect the state of every node n_i on the *Maritime* actor's Network N_{target}, impacting the nodes' confidentiality, availability, and integrity properties.

A cyberattack is characterized by its *Degree* and *Duration*. *Degree* $\Psi \in (0, 1)$ is the severity of a cyberattack over a *Maritime* actor's network, generating technical or/and business impacts. *Duration* $\delta \in (0, 1)$ refers to the length of time during which the cyberattack persists or remains active, starting from the initiation of the attack until the attack is successfully mitigated, contained, or terminated. *Duration* can vary widely depending on factors, such as the type of attack and the effectiveness of security controls, and a longer duration may result in increased damage or loss.

According to the definition of the states of SERDUX-MARCIM, *Susceptible* (S), *Exposed* (E), and *Resistant* (R) refer to states where the node does not experience the effects of the cyberattack. This is due to a *Susceptible* node has not been attacked yet, a *Exposed* node is probably infected, but due to the cyberattack has not been activated, such node is not suffering any of the cyber effects, and a *Resistant* node already has immunity to the attack.

Determining the impact of a cyberattack is crucial for distinguishing between offensive campaigns and profiling the threat agent. An effective way to evaluate this impact was proposed by Jabbour and Poisson [27] through the five D5 effects: Disrupt, Deny, Degrade, Destroy, and Deceive. The adoption of the D5 model was driven by its established use in military strategy, particularly in cyberspace

Table 6 Node's states defined in SERDUX-MARCIM model

State	Name	Description
S	*Susceptible*	Node that has a particular vulnerability level at the application, operative system, or network layer that makes it vulnerable against a specific threat. e.g., a seaport's server having vulnerabilities at the application and OS levels, making him susceptible to a targeted cyberattack
E	*Exposed*	Node that had contact with an attacked node in any of its states (Degraded, Unavailable, Destroyed) and may also be compromised. e.g., a crane system that was compromised by a cyberattack, exposing the seaport's traffic control system
R	*Resistant*	Node with cybersecurity countermeasures that make it immune against a specific threat. e.g., a server with strong security measures that remain operational, allowing partial recovery and resumption of non-affected seaport functions
D	*Degraded*	Node with resources and services partially deteriorated by a cyberattack executed with a certain degree (Low -> Partial) and a certain duration (Short -> Permanent). e.g., a crane running only part of its functions due to a cyberattack, reducing the port's operational efficiency
U	*Unavailable*	Node in a fully inoperative state by a cyberattack executed with a certain degree (Partial -> Total) and a certain duration (Short -> Temporary). The decision of the node administrator can also achieve this state. e.g., a cargo management system completely disabled due to a cyberattack, halting all port operations and cutting off communications with operational units
X	*Destroyed*	Node in a fully inoperative and unrecoverable state by a cyberattack executed with a certain degree (Partial -> Total) and a certain duration (Persistent -> Permanent). e.g., a logistic server is permanently destroyed, leading to irrecoverable data loss and the inability to automate cargo operations

operations. This approach is based on historical frameworks such as the Office of Strategic Services (OSS) Simple Sabotage Field Manual [41]. It is supported by more recent works, including Countering Cyber Sabotage by Bochman and Freeman [42], as well as MITRE's Assessment of Operational Energy System Cybersecurity Vulnerabilities [28], which provide a methodology for assessing cybersecurity risks in distributed information systems, helping organizations gauge their preparedness against cyber threats. These sources underscore the D5 model's relevance in managing cyber risks within critical infrastructures, which aligns with the military-oriented cyberdefense focus of this proposal. By employing the D5 framework in SERDUX-MARCIM model, we aim to effectively model the state transitions of nodes under cyberattack, and the association between node's states, cyberattack effects, cyberattack duration, and cyberattack duration when an attacker successfully exploits a vulnerability that seeks to generate an effect over the node.

Thus, the D5 effects and scheme were taken from this methodology to categorize the effects in terms of severity (degree) and duration. In this sense, *Degraded* (D), *Unavailable* (U), and *Destroyed* (X) refer to states where the node is suffering any of the D5 effects of a cyberattack, i.e., disrupted, degraded, denied, destroyed, or deceive, depending on the *Degree* and *Duration* of the cyberattack. Table 7 describes the association between states *Degraded* (D), *Unavailable* (U), and *Destroyed* (X), and the D5 effects. A node in the state *Degraded* D will suffer a *disrupted*, *degraded* or *Deceive* effect. A node in the state *Unavailable* (U) suffers a *denied* or *Deceive* effect. A node in the state *Destroyed* (X) suffers a *destroyed* or *Deceive* effect.

Table 7 Association between states D, U, X, and the D5 cyberattack effects

State	Cyberattack			
	Degree	Duration	Effect	
D - Degraded	$\leq 0,5$	$\leq 0,5$	Disrupted	Deceived
		$> 0,5$	Degraded	
U - Unavailable	$> 0,5$	$\leq 0,5$	Denied	
X - Destroyed		$> 0,5$	Destroyed	

4.3 Transitions between states

Every node with a particular vulnerability level becomes *Susceptible* (S), which makes it vulnerable against a specific

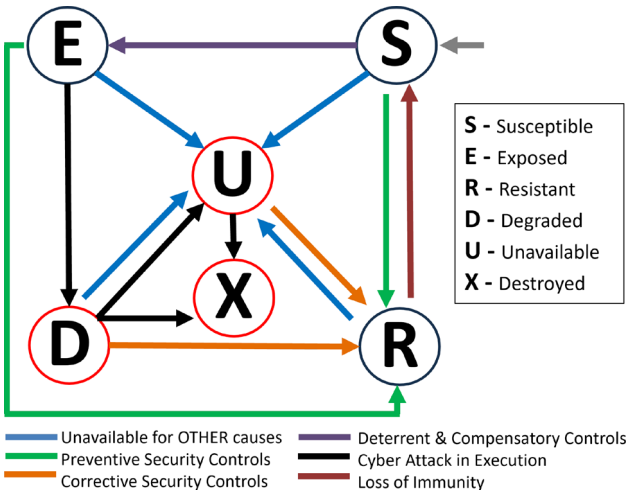


Fig. 6 Transitions between states in SERDUX-MARCIM model

threat. When a susceptible node has contact with a node under cyberattack, it becomes *Exposed* (*E*).

When the cyberattack executed its functionality over a node in *Exposed* (*E*) state, it is considered under cyberattack and becomes *Degraded* (*D*) at the beginning (regardless of the cyberattack effect), and depending on the cyberattack characteristics, *Degree* and *Duration*, it can evolve on *Unavailable* (*U*), or *Destroyed* (*X*).

A node in states *S*, *E*, *D* or *U* could become in *Resistant* (*R*) state when it has the necessary countermeasures to be immune to a specific threat or when it has received the required cybersecurity countermeasures to make it immune to a particular threat.

Additionally, nodes in states *S*, *E*, *D* or *R* could become in *Unavailable* (*U*) state due to factors that are not directly related to a cyberattack, including the decision of a node's administrator to turn it off as a measure to counter the spread of an attack.

Figure 6 shows the SERDUX-MARCIM conceptual and flow model with possible state transitions. The transitions between states mainly depend on the evolution of the cyberattack, which is highly dependent on the behavior of the cyberattack, the activation of the target/attacker's cyber capabilities, and network characteristics.

To further clarify the states and transitions proposed in the SERDUX-MARCIM model, we conducted a comparative analysis between typical phases of a cyberattack and the approach introduced by the proposed model. For this purpose, we employed the seven phases of the Cyber Kill Chain methodology [43] to illustrate how these phases are embedded within the states defined by SERDUX-MARCIM under the framework of compartmental models in epidemiology at the system level. This comparison provides insights into the dynamics of cyberattacks without delving into specific attack techniques or stages that are beyond the scope of our analysis. It allows for a comprehensive understanding of how a cyberattack evolves and impacts both the network and individual nodes, from reconnaissance to its outcomes. The results are shown in Table 8

To conduct a cyberattack analysis, for the initial condition of the *Maritime* actor's network nodes, it is assumed that the entire network is *Susceptible* (*S*) and the initial number of *Exposed* (*E*) and *Degraded* (*D*) nodes are defined by the experimenter. Table 17 summarizes the reference conditions for state transitions.

5 Cyber risk approach in SERDUX-MARCIM

A Cyber Risk Approach was established to calculate a risk value during a simulation developed using the model. The Maritime Cyberdefense Capability Model and Maritime Cyberdefense Actors Taxonomie from MARCIM project [25], together with IMO Guidelines on maritime cyber risk management [17] was taken as a reference to manage cyber risks across critical systems affecting maritime operations, and to establish the hierarchical organization of variables, particularly to define the *Target Likelihood* (λ).

Additionally, the cyber risk approach incorporates two widely recognized principles and frameworks in the field of cybersecurity: OWASP Risk Rating Methodology [26], and ISACA's security control categorization [29] [30], both of them introduced in Sect. 2.2. On one hand, OWASP Risk Rating Methodology was incorporated into our framework due to its attacker-centric approach, which provides valuable insights into maritime cyberdefense. The absence of OWASP references within the maritime domain presents an opportunity to integrate this well-established methodology into our proposal, especially given its relevance to the broader context of cyberdefense and the military's use of capabilities in cyberspace.

In our model, the interaction triad of Objective – Attacker – Cyberattack (Fig. 5) plays a critical role, which is closely aligned with the OWASP Risk Rating Methodology, due to the last one defines key elements such as: Threat Agent Factors, Vulnerability Factors, Technical Impact Factors, and Business Impact Factors. In addition, the OWASP Risk Rating Methodology contributes to establishing the hierarchical organization of variables, and particularly to calculating the variables *Attacker Likelihood* ($\aleph$) and *Cyberattack Degree* (Ψ). These variables are crucial for determining both the likelihood of a specific vulnerability being uncovered and exploited by an attacker and the impact of a successful attack. OWASP Risk Rating Methodology was also used to determine the heat matrix to assess the cyberattack severity, i.e., the severity of the risk.

On the other hand, ISACA is globally recognized as an authority in information systems audit, control, and security,

Table 8 Relationship between cyber kill chain phases and SERDUX-MARCIM states

Cyber kill chain phase	Relationship with SERDUX-MARCIM states
Reconnaissance	In this phase, the nodes belonging to the target's network are in state *Susceptible* (S), and vulnerabilities at the application, operating system, or network layer are identifiable. No compromise has yet occurred
Weaponization	The creation or acquisition of a malicious payload corresponds to nodes still being in the state *Susceptible* (S). No exposure or infection has occurred, although future exposure is possible
Delivery	As the cyberattack is transmitted to the target, nodes transition from state *Susceptible* (S) to *Exposed* (E) after contact with an attacked node. These nodes may be compromised, even if the symptoms are not visible
Exploitation	Exploitation marks the start of malicious activity. Nodes in the state *Exposed* (E) transition to *Degraded* (D) if the cyberattack causes partial degradation of resources and services. The severity depends on the cyberattack's degree and duration
Installation	The cyberattack is embedded in the system. Nodes in states *Exposed* (E) or *Degraded* (D) may transition to *Unavailable* (U) if rendered inoperative, either partially or fully, by the cyberattack or administrative decisions
Command and Control	Once attackers establish control, nodes in states *Degraded* (D) or *Unavailable* (U) may remain vulnerable. If the cyberattack is sufficiently severe, nodes may transition to state *Destroyed* (X), representing irreversible damage
Actions on Objectives	Attackers achieve their goals, such as data exfiltration or service disruption. Nodes may be in state *Degraded* (D), *Unavailable* (U), or *Destroyed* (X), depending on the cyberattack's success and its impact. Nodes in the state *Destroyed* (X) are unrecoverable

Table 9 Heat matrix to assess Cyberattack Severity

Risk Cyberattack Severity (R) Assessment				
Impact (I)	**High**	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	**Medium**	**High**
Level of Risk Cyberattack Severity (R)		**Likelihood (L)**		
		Low	**Medium**	**High**
Value		0 to < 0.3	0.3 to < 0.7	0.7 to 1

with that are widely respected frameworks and principles, particularly for their focus on governance and risk management. Thus, applying ISACA control categorization in the maritime context presents a strategic opportunity to enhance our model by incorporating best practices from other industries. This decision aligns with our broader goal of strengthening maritime cyberdefense by leveraging established and proven frameworks widely recognized for their effectiveness in cybersecurity.

In conclusion, ISACA's security control categorization was selected for SERDUX-MARCIM because it is both appropriate and essential for the cybersecurity and cyberdefense context of our study. This categorization allowed us to represent the system's dynamic nature by influencing the mathematical rates used in the differential equations, particularly when modeling different levels of security control implementation. This approach, combined with factors such as target capabilities, attacker capabilities, and the specific characteristics of each cyberattack, provided a comprehensive foundation for our model. Such an approach contributes to establishing *Likelihood Reduction Controls* (ι) and *Impact Reduction Controls* (Γ), which define the countermeasures to asset protection and determining the reduction of the likelihood or impact of a cyberattack i.e., it was taken from the methodology the security controls categorization, characteristics, and relations.

5.1 Variables and assessment

To develop the Cyber Risk Approach for the proposed model, a hierarchical organization of variables into four levels of discrimination was established, as represented in Table 10. In this table, variables at a specific level are used to calculate variables at the next upper level, e.g., variables at level 4 are used to calculate variables at level 3, and variables at level 3 are used to calculate variables at level 2. Additionally,

Table 18 and Table 19 contain the complete list of variables for SERDUX-MARCIM model, including the general meaning or question and the referent values for its assessment.

5.2 Risk cyberattack severity *R*

The general approach of the SERDUX-MARCIM model is based on the OWASP Risk Rating Methodology [26], which calculates *Risk* (R) from *Attack Likelihood* (L) and *Attack Impact* (I), as indicated in Eq. 4. The heat matrix used to compute and interpret the overall risk severity is depicted in Table 9, taking into account the risk assessment established by OWASP [26], where R, L, and $I \in (0, 1)$, taking into account that all variables in SERDUX-MARCIM were established using this range of values.

$$R = L \cdot I \tag{4}$$

Additionally, the Cyber Risk Approach in SERDUX-MARCIM considers three main components: *Target*, which refers to the *Maritime Actor*, according to Sect. 4; and *Attacker*, which refers to the *Cyber Threat Actor*; and *Cyberattack*, which represents how the *Attacker* interacts with the *Target* from an offensive perspective.

5.3 Cyberattack likelihood *L*

The ***Cyberattack Likelihood*** (L) represents the probability of the cyberattack based on some characteristics of the attacker, i.e., *Attacker Likelihood* ($\aleph$), and some characteristics of the target, i.e., *Target Likelihood* (λ). *Cyberattack Likelihood* (L) is calculated by Eq. 5, which includes the parameter $l \in (0, 0.5)$ defined by the experimenter to control the influence of *Target Likelihood* (λ) in the reduction of L. e.g., in a naval port, the *Cyberattack Likelihood* (L) of a cyberattack on the fleet's operational management system increases due to the presence of an Advanced Persistent Threat (APT) actor with significant capabilities. i.e. a high *Attacker Likelihood* ($\aleph$), and the port's reliance on outdated cybersecurity protocols, i.e. a low *Target Likelihood* (λ).

$$L = \aleph - l \cdot \lambda, \in (0, 1) \tag{5}$$

Regarding the attacker characteristics, the ***Attacker Likelihood*** ($\aleph$) represents the cybernetic capacities of an attacker to perform a hostile activity, i.e., *Attacker Factors* (ATF), and to exploit a specific vulnerability, i.e., *Vulnerability Factors* (VUF). Thus, *Attacker Likelihood* ($\aleph$) is calculated by Eq. 6.

$$\aleph = \frac{ATF + VUF}{2}, \in (0, 1) \tag{6}$$

Recognition of the threat agent is essential to understand the magnitude of the risk, that is why OWASP [26] indicates that the estimation of the ***Attacker Factors*** (ATF) should consider different dimensions like the attacker's technical skills, i.e., *Skill Level* (SKL), the grade of motivation of the attacker to exploit the vulnerability, i.e., *Motive* (MOT), the availability of resources on in the attacker side, i.e., *Opportunity* (OPP), and the number of members affiliated with the attacker, i.e., *Size* (SIZ). Thus, *Attacker Factors* (VUF) is calculated by Eqs. 7.

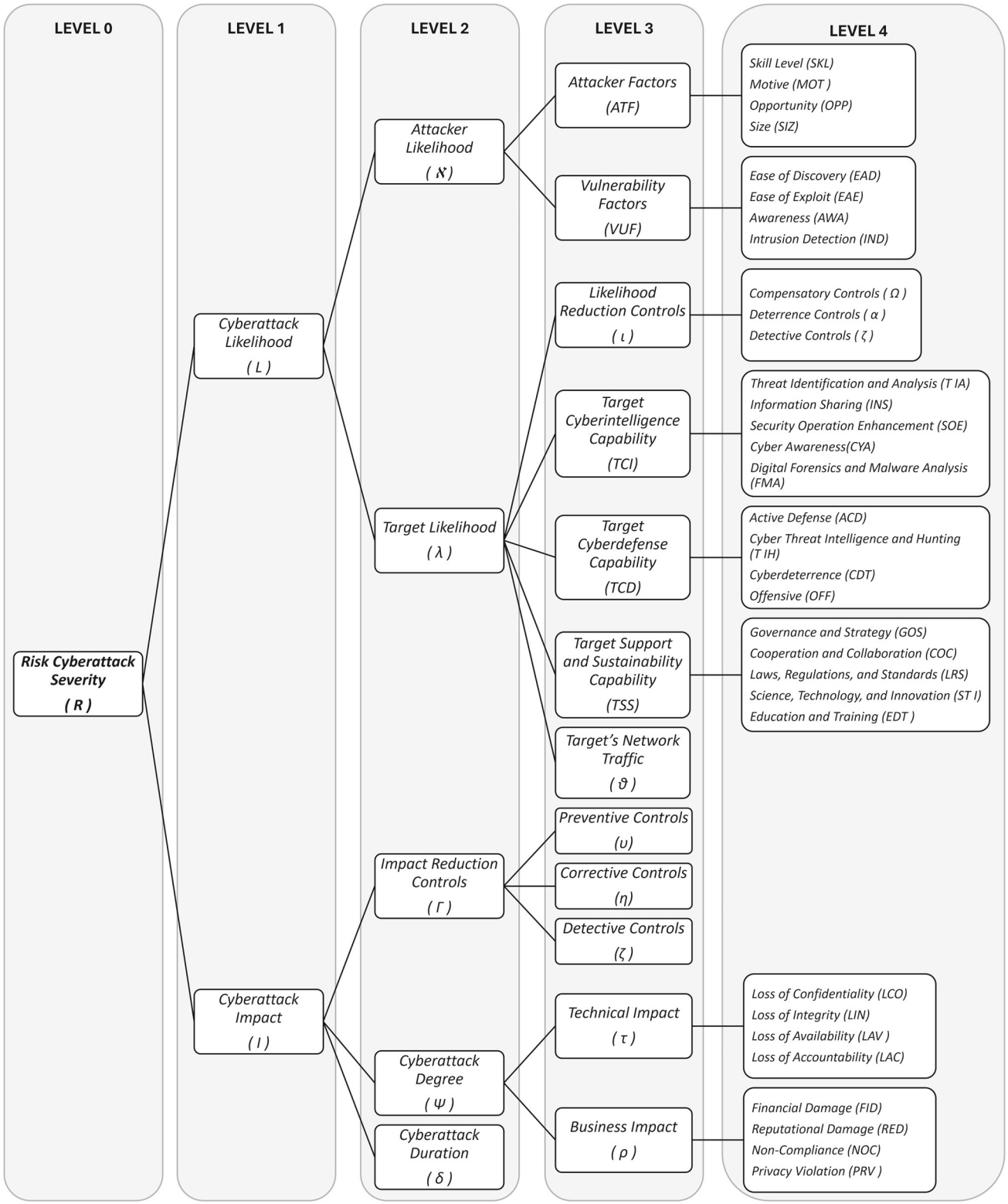
$$ATF = \frac{SKL + MOT + OPP + SIZ}{4}, \in (0, 1) \tag{7}$$

In addition, to recognize the capacities of the adversary, it is also important to understand the nature of the vulnerability that the adversary could exploit; that is why OWASP [26] indicates that the estimation of the ***Vulnerability Factors*** (VUF) should consider different vulnerability-associated features like ease of the attacker to find the vulnerability, i.e., *Ease of Discovery* (EAD), the easiness for the attacker to exploit the vulnerability, i.e., *Ease of Exploit* (EAE), the popularity of the vulnerability, i.e., *Awareness* (AWA), and the probability of detecting the vulnerability exploitation, i.e., *Intrusion Detection* (IND). Thus, *Vulnerability Factors* (VUF) is calculated by 8.

$$VUF = \frac{EAD + EAE + AWA + IND}{4}, \in (0, 1) \tag{8}$$

Regarding the target characteristics, ***Target Likelihood*** (λ) represents the cybernetic capacities of the victim organization to react to the cyberattack, which according to the "Cyberdefense Capabilities Model" defined by MARCIM [25] should consider: the security controls deployed in the organization that avoids the occurrence of the cyberattack, i.e., *Likelihood Reduction Controls* (ι), the capacity of the organization to collect, process, and use intelligence information, i.e., *Target Cyberintelligence Capability* (TCI), the capacity of the organization to plan and execute offensive actions in the occurrence of a cyberattack, i.e., *Target Cyberdefense Capability* (TCD), and the capacity of the organization to maintain a coordinated and systematic response against cyberattacks, i.e., *Target Support and Sustainability Capability* (TSS). Thus, the *Target Likelihood* (λ) is calculated by Equation 9. In this equation, w_1, w_2, w_3, and w_4 are weights defined by the experimenter depending on the scenario simulated to control how each target capability influences λ.

Table 10 Hierarchical organization of variables for the Cyber Risk Approach for SERDUX-MARCIM



$$\lambda = w_1 \cdot \iota + w_2 \cdot TCI + w_3 \cdot TCD + w_4 \cdot TSS - \theta$$
$$\lambda \in (0, 1)$$
$$\sum_{n=1}^{4} w_n = 1 \tag{9}$$

The estimation of ***Likelihood Reduction Controls*** (ι) was done considering the ISACA [29] definition of controls shown in Sect. 2.2 that indicates that the likelihood of an attack is reduced with *Compensatory* (Ω), *Deterrence* (α) and *Detective* (ζ) controls. *Likelihood Reduction Controls* (ι) is calculated by Eq. 10.

$$\iota = \frac{3}{\frac{1}{\Omega} + \frac{1}{\alpha} + \frac{1}{\zeta}}, \in (0, 1) \tag{10}$$

The definition of ***Target Cyberintelligence Capabilities*** (TCI) was primarily informed by the foundational works of references [44–47] and [48]. The authors also leveraged their extensive professional experience to refine and enhance variables related to the use of information regarding cyber threats and vulnerabilities to protect digital assets and data. In this sense, TCI integrates specific capacities of the victim organization to discover threats, i.e., *Threat Identification and Analysis* (TIA), to sustain an information sharing scheme, i.e., *Information Sharing* (INS), to empower cyber operations with intelligence information, i.e., *Security Operation Enhancement* (SOE), to educate own personal in cybersecurity risks, i.e., *Cyber Awareness* (CYA), to plan and execute a cyberforensic cycle, i.e., *Digital Forensics and Malware Analysis* (FMA). Thus, *Target Cyberintelligence Capability* (TCI) is defined by Eq. 11.

$$TCI = \frac{TIA + INS + SOE + CYA + FMA}{5}$$
$$TCI \in (0, 1) \tag{11}$$

On the other hand, the ***Target Cyberdefense Capability*** (TCD) was developed with primary insights drawn from the seminal works of references [44, 49] and [50]. In addition, the author's extensive professional experience provided crucial practical insights that influenced the variables related to the strategies and measures an organization employs to protect its digital assets, systems, and data from cyber threats. In this sense, TCD considers different defensive capacities of the victim organization: the capacity to deploy defensive measures to avoid a cyberattack, i.e., *Active Defense* (ACD), the capacity to develop threat intelligence cycles, i.e., *Cyber Threat Intelligence and Hunting* (TIH), the capacity to discourage the enemy from starting a cyberattack, i.e., *Cyberdeterrence* (CDT), and the capacity to conduct offensive cyber operation i.e., *Offensive* (OFF). The *Cyberdeterrence* (CDT) and *Offensive* (OFF) capabilities should be considered only for actors with the legal attributions and resources to conduct such activities, e.g., a military cyber command. Thus *Target Cyberdefense Capability* (TCD) is defined by Eq. 12, which considered $cond = 0$ for situations where the victim organization has legal attributions that allow him to use *Cyberdeterrence* (CDT) and *Offensive* (OFF) capabilities. In other cases, $cond = 1$.

$$TCD = d_1 ACD + d_2 TIH + d_3 CDT + d_4 OFF, \in (0, 1)$$
$$where, \sum_{n=1}^{4} d_n = 1, \quad cond = 0$$
$$or, d_1 + d_2 = 1 \quad and \quad d_3, d_4 = 0, \quad cond = 1 \tag{12}$$

At last, ***Target Support and Sustainability Capability*** (TSS) was deeply rooted in the foundational research of [21, 44, 51, 52] and [53], and was further shaped by the author's professional expertise to define the variables around the development and maintenance of robust cyber support systems aimed at ensuring long-term operational resilience and efficiency, to protect and sustain digital infrastructure and services over time. In this sense, TSS is composed of the abilities of the victim organization to maintain a cybersecurity governance structure, i.e., *Governance and Strategy* (GOS), the ability to cooperate efficiently, i.e., *Cooperation and Collaboration* (COC), the capacity to follow cybersecurity associated laws, i.e., *Laws, Regulations, and Standards* (LRS), the ability to innovate cybersecurity practices, i.e., *Science, Technology, and Innovation* (STI), and the ability of the organization to maintain a defined cybersecurity and cyberdefense education plan, i.e., *Education and Training* (EDT). Thus, *Target Support and Sustainability Capability* (TSS) is defined by Eq. 13.

$$TSS = \frac{GOS + COC + LRS + STI + EDT}{5}$$
$$TSS \in (0, 1) \tag{13}$$

The ***Target's Network Traffic*** (θ) is a variable to reduce the value of *Target Likelihood* (λ) depending on the robustness of the network. The higher the *Number of Node Connections* (nl) in N is, the higher the complexity of a target to counter a cyberattack. In this sense, Eq. 14 calculates *Target's Network Traffic* (θ) considering that a highly connected network occurs when $nl \geq \frac{N}{10}$, and the maximum penalty due to the network traffic is 0.1, i.e., 10%, over the total value of *Target Likelihood* (λ).

$$\theta = \min\left(\frac{nl}{(N-1)}, 0.1\right), \in (0, 0.1) \tag{14}$$

5.4 Cyberattack impact *I*

The ***Cyberattack Impact*** (I) represents of the damage of the cyberattack based on the capacity of the victim organization to reduce the damage, i.e. *Impact Reduction Controls* (Γ), the operative impact of the cyberattack, i.e. *Cyberattack Degree* (Ψ), and the duration of the offensive campaign against the target, i.e. *Cyberattack Duration* (δ). e.g., following a successful breach of a naval port's management system, the overall *Cyberattack Impact* (I) would be determined by the affectation to port operations, i.e. a high *Cyberattack Degree* (Ψ), the sustained duration of the attack, i.e. a long *Cyberattack Duration* (δ), and by the effectiveness of the port's countermeasures, i.e. a strong *Impact Reduction Controls* (Γ), such as rapid system backups or manual overrides.

$$I = \frac{\Psi + \delta}{2} - i \cdot \Gamma, \in (0, 1) \tag{15}$$

The ***Impact Reduction Controls*** (Γ) allows understanding the maturity of the victim organization in terms of the adoption of the 3 categories of controls that, according to ISACA [29], avoid the occurrence of a cyberattack, i.e., *Preventive Controls* (υ), the ability to detect an ongoing cyberattack, i.e., *Detective Controls* (ζ), and the capacity to remediate assets impacted by a cyberattack, i.e., *Corrective Controls* (η).

$$\Gamma = \frac{3}{\frac{1}{\eta} + \frac{1}{\upsilon} + \frac{1}{\zeta}}, \in (0, 1) \tag{16}$$

The ***Cyberattack degree*** (Ψ) enables an understanding of a cyberattack's technological and business affectation. According to OWASP [26], *Cyberattack Degree* (Ψ) should be evaluated considering the direct impact on the technological infrastructure, i.e., *Technical Impact* (τ), and considering the impact on a business that goes beyond the technical component and includes financial, reputation, and legal aspects, i.e., *Business Impact* (ρ).

$$\Psi = \frac{(\tau + \rho)}{2}, \in (0, 1) \tag{17}$$

$$\tau = \frac{LCO + LIN + LAV + LAC}{4}, \in (0, 1) \tag{18}$$

$$\rho = \frac{FID + RED + NOC + PRV}{4}, \in (0, 1) \tag{19}$$

The ***Cyberattack Duration*** (δ) considers a 0 to 1 scale to represent the duration of a cyberattack with four reference values in a discrete scale: Short-term (0.25), Temporary (0.5), Persistent (0.75), or Permanent (1).

6 System of differential equations in SERDUX-MARCIM

SERDUX-MARCIM proposes time-dependent transition rates, that consider the actions taken by the target, i.e., the maritime actor, to prepare for and counter the cyberattack generated by the attacker, i.e., the cyber threat actor, which influences the outcome over time. Thus, the system of differential equations proposed in SERDUX-MARCIM for modeling a cyberattack is shown in Eq. 20.

$$\begin{cases} \frac{dS}{dt} = \Lambda + \omega R - \beta S - \mu S - \phi S \\ \frac{dE}{dt} = \beta S - \sigma E - \mu E - \phi E \\ \frac{dR}{dt} = \gamma D + \gamma U + \phi S + \phi E - \omega R - \mu R \\ \frac{dD}{dt} = \sigma E - \gamma D - \mu D - \nabla D - \chi D \\ \frac{dU}{dt} = \mu(S + E + D + R) + \nabla D - \chi U - \gamma U \\ \frac{dX}{dt} = \chi D + \chi U \end{cases} \tag{20}$$

where,

- $\beta(t)$ is the *Propagation Rate*
- $\sigma(t)$ is the *Cyberattack (Degraded) Rate*
- $\gamma(t)$ is the *Recovery Rate*
- $\phi(t)$ is the *Sanitation Rate*
- $\omega(t)$ is the *Loss of Resistance Rate*
- $\nabla(t)$ is the *Cyberattack (Unavailable) Rate*
- $\chi(t)$ is the *Cyberattack (Destroyed) Rate*
- $\mu(t)$ is the *Unavailability by Other Causes Rate*

In the previous equation, $\beta(t), \sigma(t), \gamma(t), \phi(t), \omega(t), \nabla(t), \chi(t)$, and $\mu(t)$ are transition rates that define the state changes for each node in the network N. To facilitate the understanding of these transition rates, Fig. 7 points out the relation between each rate defined in the current section and the states' transitions defined previously in Sect. 4.2. Each one of the previously proposed time-dependent rates will be described next, including for each one an hypothetical example in the context of maritime cybersecurity and cyberdefense. Such examples are intended to demonstrate how the proposed rates could be applied in maritime scenarios, but do not refer to a documented real incident.

6.1 Propagation rate β

The rate measures the speed at which a cyberattack spreads through a network. This rate takes into account all nodes in the state *Susceptible* (S) that transit to the state *Exposed* (E) due to their contact with an infected node that is in the state

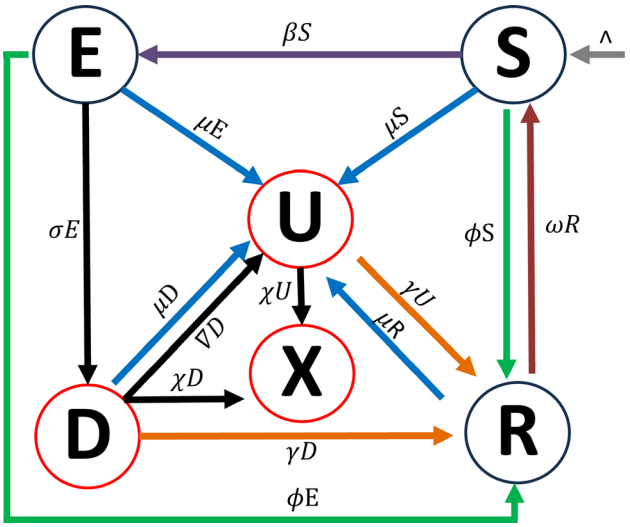


Fig. 7 Association between the transition rates and the changes of state for SERDUX-MARCIM

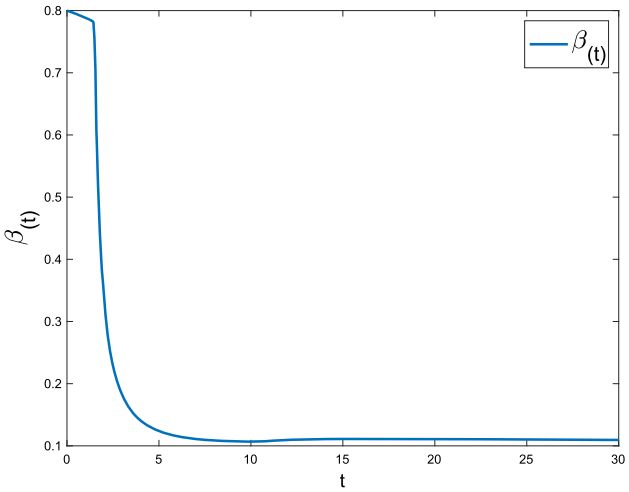


Fig. 8 *Propagation Rate* ($\beta(t)$) when $\beta_0 = 0.8$ and $\xi = 0.6$

Degraded (D), *Unavailable* (U), or *Destroyed* (X). Essentially, *Propagation Rate* (β) shows how quickly a cyberattack can reach susceptible nodes in a network.

The *Propagation Rate* (β) is expressed in Eq. 21, which allows to represent a scenario where there is an initially increasing number of infected nodes as the cyberattack spreads. This decreases because there will be fewer nodes prone to infection. This rational function was chosen because it captures both the peak infection phase and the subsequent decay, ensuring that the propagation rate remains bounded and asymptotically approaches zero as the number of infected nodes increases.

$$\beta_{(t)} = \frac{\beta_{(0)}}{1 + (1 - \xi)(D(t) + U(t) + X(t))}, \in (0, 1) \quad (21)$$

$$\xi = \frac{2}{\frac{1}{L} + \frac{1}{\Psi}} \quad (22)$$

In Eq. 21, $\beta_{(0)}$ is the *Initial Propagation Rate*; N is the *Total Population Size* in the network; expression $D(t) + U(t) + X(t)$ groups all nodes in states *Degraded* D, *Unavailable* U and *Destroyed* X in a moment t; Finally, ξ is a parameter calculated by Eq. 22, which is used to establish the decay speed of $\beta(t)$, and depends on the *Cyberattack Likelihood* (L) and the *Cyberattack Degree* (Ψ) defined in Sect. 5. A harmonic mean function was selected to represent ξ because of the proportional relationship between *Cyberattack Likelihood* (L) and *Cyberattack Degree* (Ψ).

A representation of the *Propagation Rate* (β) shows that the rate decreases over time, as shown in Fig. 8. In such figure, the number of nodes in states *Degraded* (D), *Unavailable* (U) and *Destroyed* (X) was 40% of the total amount of nodes available in the network, *e.g.,* consider a scenario where a naval fleet deployed in the Caribbean that becomes the target of a sophisticated cyberattack aimed at the *Automatic Identification System (AIS)*–a critical maritime data transmission system widely used for navigational safety. This system allows vessels to transmit their positions and receive information from other ships to avoid collisions. In this scenario, the cyberattack initially compromises the AIS of a single vessel. From there, the infection propagates to other systems within the vessel and subsequently distributions to interconnected vessels via shared communication networks. The *Propagation Rate* $\beta(t)$ quantifies the speed at which the infection transitions vessel systems (nodes) from the *Susceptible* (S) state, representing systems that are yet unaffected, to the *Exposed* (E) state, indicating systems that show early signs of compromise. This example underscores the domino effect of cyber threats in maritime environments and highlights the critical need for robust defenses to mitigate such propagation risks.

6.2 Cyberattack (degraded) rate σ

This time-dependent rate refers to the speed at which a cyberattack occurs in a network. It determines the transition of nodes from state *Exposed* (E) to *Degraded* (D). Cyberattack campaigns exhibit different behaviors and do not follow a static pattern over time. e.g., malware can infect several nodes, then become dormant, and at some point get activated again due to receiving instructions from a command and control server.

The *Cyberattack (Degraded) Rate* (σ) is calculated by Eq. 23 which is composed by an *Initial Phase* and *Final Phase*. The reason for having two phases is that in the *Initial Phase*, the infection is spread along the nodes at a certain

speed that depends on the capacity of the victim organization to detect and prevent it. In the *Final Phase*, the infection is detained at a certain speed that depends on the capacity of the victim organization to react and correct the cyberattack.

$$\sigma(t) = Phase_{Initial}(t) + Phase_{Final}(t), \in (0, 1) \tag{23}$$

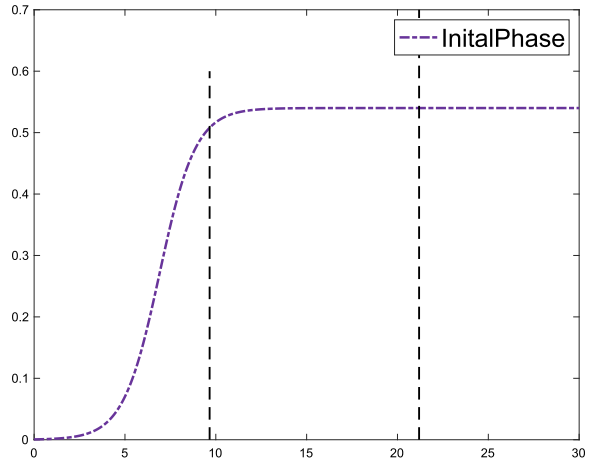
A sigmoid function was selected to represent the *Initial* and *Final Phase* because it offers a smooth curve with an activation property that allows it to describe the moment at which the cyberattack is activated or contained. The *Initial Phase* is calculated through Equation 24. The height of the sigmoid function is given by $(1 - \Gamma) \cdot \Psi$, indicating that for higher values of *Impact Reduction Controls* (Γ), the height of the sigmoid function decreases. The *Likelihood Reduction Controls* (ι) parameter controls the smoothness of the *Initial Phase*. The expression $-t_f * \Theta + t_f/4$ denotes the sigmoid activation point, where parameter t_f corresponds to the final simulation time. Thus, the $tf/4$ value indicates that there are two activation points in SERDUX-MARCIM, the first at $t_f/4$ and the second at $3t_f/4$. In addition, $\Theta = \delta \cdot (1 - \Gamma)$ represents the width of the active interval.

$$Phase_{Initial}(t) = \frac{(1 - \Gamma) \cdot \Psi}{1 + e^{-\iota\left(t - t_f \cdot \Theta + \frac{t_f}{4}\right)}}, \in (0, 1) \tag{24}$$

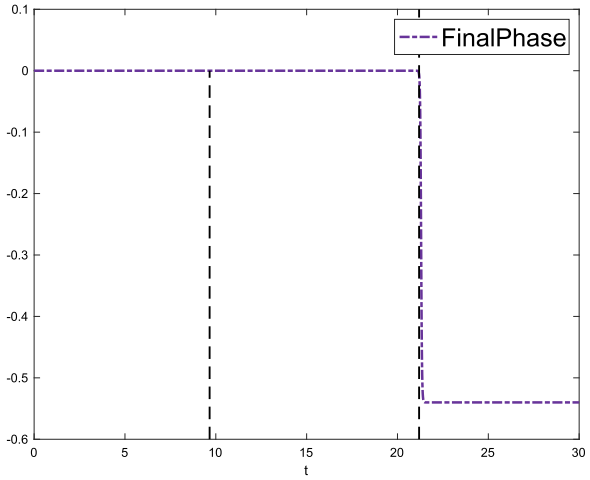
The *Final Phase* is calculated through Eq. 25. It is a negative sigmoid function because it has an opposite behavior to the *Initial Phase*. The drop rate is controlled by the variable *Impact Reduction Controls* (Γ). The end of the interval is represented by $-t_f \cdot \Theta + t_f/4 - t_f \cdot \Theta$.

$$Phase_{Final}(t) = -\frac{(1 - \Gamma) \cdot \Psi}{1 + e^{-\Gamma\left(t - t_f \cdot \Theta + \frac{t_f}{4} - t_f \cdot \Theta\right)}}, \in (0, 1) \tag{25}$$

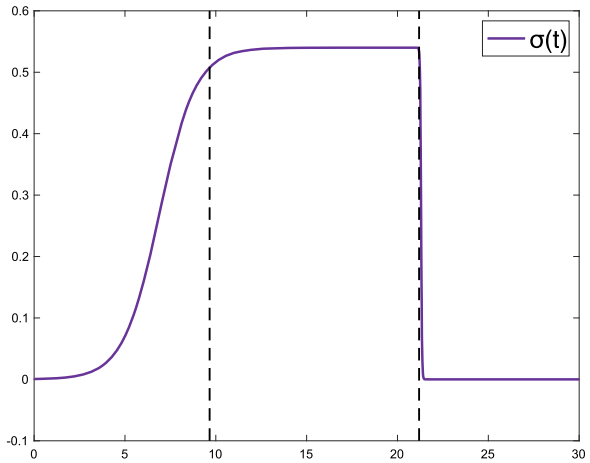
A graphic representation of the *Cyberattack (Degraded) Rate* (σ) is shown in Fig. 9, which is the sum of the two sigmoid functions defined in the *Initial* and *Final Phase*. The parameters used to obtain such figure were *attack duration* (δ) with a value of 0.8, *Impact Reduction Controls* (Γ) of 0.4, *Attack Degree* (ψ) of 0.9 and *Final Time of Simulation*(t_f) of 30 units of time, *e.g.,* as the cyberattack progresses, some vessels experience partial degradation in their systems and operational capabilities. For instance, the compromised AIS begins transmitting incorrect positional data, which affects dependent systems such as electronic charts and onboard navigation systems. The *Cyberattack (Degraded) Rate* $\sigma(t)$ represents the rate at which vessel systems transition from an operational state to a *Degraded* (D) state due to the interference caused by the cyberattack.



(a) *InitialPhase*



(b) *FinalPhase*



(c) $InitialPhase + FinalPhase = \sigma(t)$

Fig. 9 Composition of the *Cyberattack (Degraded) Rate* $\sigma(t)$

6.3 Cyberattack (unavailable) rate ∇

This rate defines the transition of nodes toward the state *Unavailable* (U), which occurs when an attack, with a *Cyberattack Degree* $\Psi \geq 0.5$ and *Cyberattack Duration* $\delta \leq 0.5$, makes nodes in states *Susceptible* (S), *Exposed* (E), *Degraded* (D) or *Resistant* (R), move to the state *Unavailable* (U), e.g., when a cyberattack corrupt critical operating system files causing the operating system of a machine become unusable.

The *Cyberattack (Unavailable) Rate* ∇ is calculated by Eq. 26, which incorporates the *Cyberattack Degree* (Ψ) and the *Cyberattack Duration* (δ) detailed in Sect. 5. The *Cyberattack (Unavailable) Rate* (∇) was defined as a piecewise function that only takes values when $\Psi \geq 0.5$ and $\delta \leq 0.5$, and 0 otherwise. This piecewise function computes the harmonic mean between *Cyberattack Degree* (Ψ) and *Cyberattack Duration* (δ). The harmonic mean function was chosen because it emphasizes that the lowest factor between *Cyberattack Degree* (Ψ) or *Cyberattack Duration* (δ) will influence the the cyberattack impact. In this manner, if one of these factors, *Cyberattack Degree* (Ψ) or *Cyberattack Duration* (δ), is very high while the other is low, the harmonic mean will be closer to the lowest value, indicating that cyberattacks with higher *Cyberattack Degree* (Ψ) and *Cyberattack Duration* (δ) will have the most impact, textite.g., in this scenario, as the cyberattack intensifies, certain vessels systems experience critical failures rendering them unavailable (U) for any operational activity. For example, the corrupted AIS causes cascading failures in the navigation system or corrupts other critical systems leading to the vessel's isolation from the fleet's operations. The *Cyberattack (Unavailable) Rate* $\nabla(t)$ captures the rate at which vessels systems transition from *Susceptible* (S), *Exposed* (E), or *Degraded* (D) states to the *Unavailable* (U) state due to the direct impact of the cyberattack. In addition, factors unrelated to a cyberattack can render other vessel systems Unavailable (U), such as OS failures or update needs. The *Cyberattack (Unavailable) Rate* $\nabla(t)$ quantifies this unavailability by other causes, highlighting the rate at which vessel systems are taken offline for reasons not directly related to the cyberattack, thus affecting the fleet's overall operational capacity.

$$\nabla(\Psi, \delta) = \begin{cases} \frac{2}{\frac{1}{\Psi}+\frac{1}{\delta}}, & \text{if } \Psi \geq 0.5 \text{ and } \delta \leq 0,5 \\ 0, & \text{otherwise} \end{cases} \tag{26}$$

6.4 Cyberattack (destroyed) rate χ

This rate applies to nodes in states *Degraded* (D) or *Unavailable* (U) with exploited vulnerabilities that allow them to transit to the state *Destroyed* (X). The attack behind this transition is generally one with a *Cyberattack Degree* $\Psi \geq 0.5$ and a *Cyberattack Duration* $\delta > 0.5$ that destroys nodes, e.g., when a cyberattack that affects physical or critical software components affecting the system at all. The *Cyberattack (Destroyed) rate* χ is calculated through Eq. 27, which considers the *Cyberattack Degree* (Ψ) and *Cyberattack Duration* (δ). Equation 27 is similar to Eq. 26 in the sense that it employs a harmonic mean function that considers both the *Cyberattack Degree* (Ψ) and the *Cyberattack Duration* (δ) to determine the cyberattack impact. However, since the *Cyberattack (Destroyed) rate* (χ) is involved twice in the transition to the *Destroyed* (X) state, due to nodes in state *Degraded* (D) or *Unavailable* (U) can migrate to state *Destroyed* (X), i.e., $\frac{dX}{dt} = \chi D + \chi U$, the computation of the harmonic mean is divided by two, *e.g.,* in severe cases, the cyberattack causes irreparable damage to some vessel systems. For instance, the navigation system and other critical systems are permanently corrupted, making recovery impossible and rendering some vessel systems in a *Destroyed* (X) state. The *Cyberattack (Destroyed) Rate* $\chi(t)$ represents the rate at which vessel systems transition from an operational state to a *Destroyed* (X) state due to the catastrophic impact of the cyberattack. This underscores the potential catastrophic consequences of a cyberattack on naval assets.

$$\chi(\Psi, \delta) = \begin{cases} \frac{1}{\frac{1}{\Psi}+\frac{1}{\delta}}, & \text{if } \Psi \geq 0.5 \text{ and } \delta > 0,5 \\ 0, & \text{otherwise} \end{cases} \tag{27}$$

6.5 Recovery rate γ

This rate applies to nodes in the state of *Degraded* (D) or *Unavailable* (U) that may adopt the necessary countermeasures to be immune against the cyberattack. It reflects the speed at which a network can respond to a cyberattack and recover nodes in the state *Degraded* (D) or *Unavailable* (U) nodes. This rate depends on the deployment of the proper corrective controls and the application of resilience plans.

The *Recovery Rate* (γ) is calculated using Eq. 28, which considers the rate behavior as a hyperbolic tangent, where expression $\frac{D(t)+U(t)+X(t)}{N}$ includes all nodes under cyberattack in states *Degraded* (D), *Unavailable* (U) and *Destroyed* (X) in a moment t. This function was selected because it ensures that *Recovery Rate* (γ) is positive, continuous over its domain, and bounded, providing in such a way a smooth transition in recovery rates and preventing unrealistic fluctuations. This expression is multiplied by 3 to ensure the hyperbolic tangent function takes values near 1. Variable $\eta \in (0, 1)$ is a Corrective Control parameter that determines how fast the *Recovery Rate* (γ) will approach 1. However, since the *Recovery rate* (γ) affects two states, *Degraded* (D) and *Unavailable* (U); thus, it is divided by 2. The *Recovery rate* (γ) is expected to initially be low and then increase depending on the *Cyberattack Degree* (Ψ) and *Cyberattack*

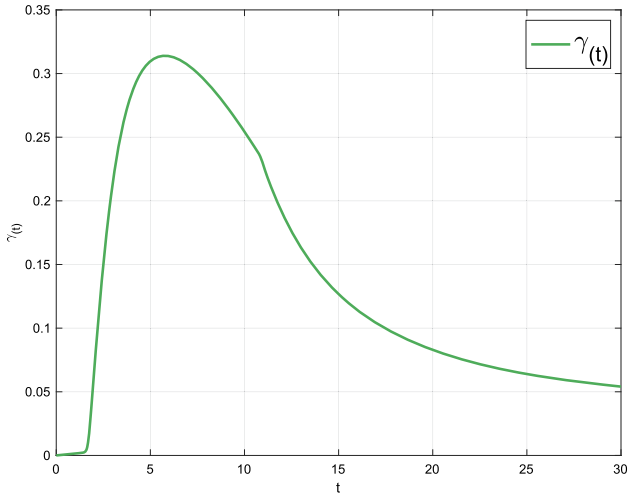


Fig. 10 *Recovery Rate* $\gamma(t)$ with $\eta = 1$

Duration (δ). In the context of a widely known attack, a set of corrective controls is expected to be activated rapidly; however, in a zero-day attack, the corrective controls will be delayed. An example of the typical behavior of *Recovery Rate* (γ) is shown in Fig. 10, when $N = 32$ is given by 30 nodes in state *Susceptible* (S) and 2 nodes in state *Exposed* (E). Parameters used to generate Fig. 10 are next: *Preventive Controls Implementation* $\upsilon = 1$, *Compensatory Controls Implementation* $\Omega = 0.5$, *Deterrence Controls Implementation* $\alpha = 0.5$, *Detective Controls Implementation* $\zeta = 0.3$, *Cyberattack Likelihood* $L = 0.6$, *Cyberattack Degree* $\Psi = 0.4$, *Cyberattack Duration* $\delta = 0.7$, $a = 0.5$, $m = 1$, *Initial Propagation Rate* $\beta_0 = 0.8$, and *Unavailability by other causes Rate* $\mu = 0.001$, *e.g.,* in response to the cyberattack, the naval fleet deploys cyberdefense teams to establish immediate countermeasures and recover affected systems. For instance, compromised systems are reconfigured, and updated software patches are applied to mitigate the damage. The *Recovery Rate* $\gamma(t)$ represents the rate at which vessel systems in *Degraded* (D) or *Unavailable* (U) states regain their functionality through recovery efforts. This recovery depends on the effectiveness of the implemented corrective measures and resilience plans activated by the fleet's cyberdefense team.

$$\gamma_{(t)} = \frac{\eta}{2} \cdot \tanh\left(\frac{D(t) + U(t) + X(t)}{N} \cdot 3\right), \in (0, 0.5) \quad (28)$$

6.6 Sanitation rate ϕ

This rate applies to nodes in the states *Susceptible* (S) and *Exposed* (E) that received cybersecurity countermeasures that make them immune against the cyberattack and transit to the state *Resistant* (R). It represents the speed at which a victim organization secures vulnerable nodes using appropriate safeguards, guaranteeing that nodes operate normally.

The *Sanitation Rate* (ϕ) is calculated using Eq. 29, which considers the rate behavior as a hyperbolic tangent where expression $\frac{S(t)+E(t)}{N}$ includes all nodes vulnerable to a cyberattack in states *Susceptible* (S) and *Exposed* (E) at moment t. This function was selected because it ensures that *Sanitation Rate* (ϕ) is positive, reflecting only favorable recovery rates in our simulation. Moreover, the hyperbolic tangent function is continuous over its domain and bounded, providing a smooth transition in recovery rates and preventing unrealistic fluctuations. This expression is multiplied by 3 to ensure the hyperbolic tangent function takes values near 1. The parameter $\upsilon \in (0, 1)$ is a *Preventive Controls Implementation* parameter that determines how fast the *Sanitation Rate* (ϕ) will approach to 1. However, since the *Sanitation Rate* (ϕ) is involved in the transition equation of two states, *Susceptible* (S) and *Exposed* (E), by reducing the number of nodes, it is divided by two. *Sanitation Rate* (ϕ) is expected to be low initially, depending on the *Cyberattack Degree*(Ψ) and the *Cyberattack Duration* (δ).

$$\phi_{(t)} = \frac{\upsilon}{2} \cdot \left(1 - \tanh\left(\frac{S(t) + E(t)}{N} \cdot 3\right)\right), \in (0, 0.5) \quad (29)$$

As the attack progresses, preventive security controls are expected to be effective in making the node resistant. However, it is likely that during the early stages of the cyberattack, most nodes will move to the state *Resistant* (R). An example of the behavior of this rate is shown in Fig. 11, when N= 32 given by 30 *Susceptible* and 2 *Exposed*. The parameters used to generate Fig. 11, are next: *Preventive Controls Implementation* $\upsilon = 1$, *Compensatory Controls Implementation* $\Omega = 0.5$, *Deterrence Controls Implementation* $\alpha = 0.5$, *Detective Controls Implementation* $\zeta = 0.3$, *Cyberattack Likelihood* $L = 0.6$, *Cyberattack Degree* $\Psi = 0.4$, *Cyberattack Duration* $\delta = 0.7$, $a = 0.5$, $m = 1$, *Initial Propagation Rate* $\beta_0 = 0.8$, and *Unavailability by other causes rate* $\mu = 0.001$, *e.g.,* to prevent further damage, the fleet initiates a sanitation process for systems identified as vulnerable. For example, vessel systems on *Susceptible* (S) and *Exposed* (E) undergo a thorough cybersecurity hardening process, applying patches and updates to their systems to prevent future vulnerabilities. The *Sanitation Rate* $\phi(t)$ captures the rate at which these vessel systems are transitioned to a *Resistant* (R) state, reducing the fleet's overall vulnerability.

6.7 Loss of resistance rate ω

The *Loss of Resistance Rate* (ω) applies to all *Resistant* (R) nodes that have lost their immunity. One reason for a loss of resistance is the instability in the countermeasure's efficiency

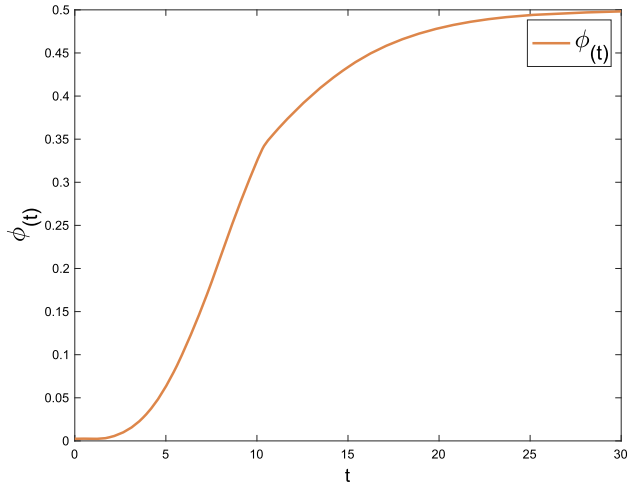


Fig. 11 *Sanitation Rate* $\phi(t)$ with $\upsilon = 1$

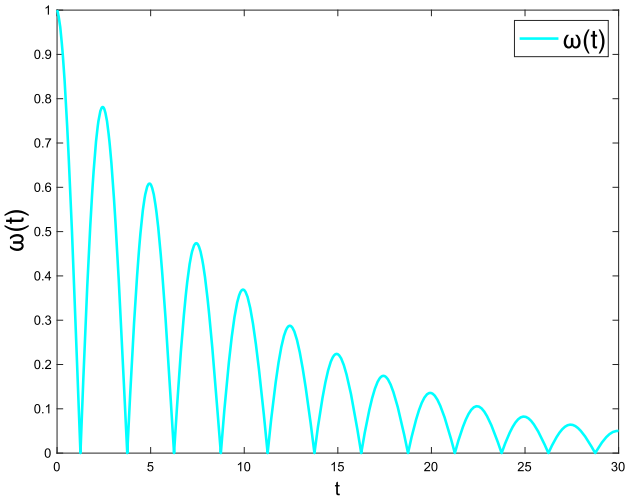


Fig. 12 Loss of resistance rate $\omega(t)$ with $a = 0.1$ and $m = 5$

that can be observed in the first stages of a cyberattack when new information about the attack comes up, e.g., variations (mutated or obfuscated) of the original sample and countermeasures become obsolete. Due to these factors, the *Loss of Resistance Rate* (ω) may fluctuate. However, it is expected that it will eventually become 0, indicating that all nodes in the network have become immune.

The behavior of the *Loss of Resistance Rate* (ω) is calculated by Eq. 30. The *Loss of Resistance* (ω) is a damped cosine function representing oscillations over time provoked by the states of the cyberattack. It considers time t and $a > 0$ as the parameters to determine the strength of the cosine damping, and $m > 0$ to control the length of the cosine period.

$$\omega_{(t)} = \left| e^{-at} \cos\left(\frac{2\pi t}{m}\right) \right|, \in (0, 1) \tag{30}$$

An example of the typical rate behavior of *Loss of Resistance Rate* (ω) is shown in Fig. 12, *e.g.,* over time, as new variants of the cyberattack are detected, even vessel systems that were initially *Resistant* (R) may experience a loss of their immunity. For instance, updates to the attack's methodology could exploit previously unknown vulnerabilities, gradually diminishing the vessel's resistance. The *Loss of Resistance Rate* $\omega(t)$ captures this process, reflecting how resistance can weaken due to evolving cyber threats, emphasizing the importance of vigilance and ongoing updates to countermeasures.

6.8 Unavailability by other causes rate μ

Factors not directly related to a cyberattack can cause nodes in states *Susceptible* (S), *Exposed* (E), *Degraded* (D) or *Resistant* (R), enter in the state *Unavailable* (U), e.g., hardware or software failures, errors in the application of patches or reconfigurations, incompatibilities between the node and the countermeasure being applied, physical incidents, human errors, or simply by the decision of a node's administrator who decides to turn it off as a measure to counter the spread of an attack. Thus, the *Unavailability by Other Causes Rate* (μ) $\in (0, 1)$ integrates those previously mentioned factors and may be typically $\mu < 0.0025$, meaning that at least 1% of the nodes in the states *Susceptible* (S), *Exposed* (E), *Degraded* (D), or *Resistant* (R) could change to state *Unavailable* (U), due to other causes. This calculation is based on the understanding that nodes originate from four sources: *Susceptible* (S), *Exposed* (E), *Degraded* (D), and *Resistant* (R), and thus, the rate is divided by 4. Additionally, to ensure that the number of unavailable nodes due to other causes remains low, a maximum of 1% is considered, from which the value 0.0025 is derived, *e.g.,* external factors unrelated to the cyberattack can also render the vessel systems unavailable. For example, hardware failures or scheduled maintenance of systems might temporarily take a vessel offline. The *Unavailability by Other Causes Rate* $\mu(t)$ captures this unavailability rate, ensuring that the analysis accounts for all potential disruptions to the fleet's operational readiness, whether they stem from the cyberattack or other causes.

6.9 New nodes rate Λ

The *New Nodes Rate* $\Lambda \in Z^+$ represents the number of new nodes added to the target's network in every time step t, which is a target's decision. When a target realizes it is being attacked, it may avoid new nodes connecting to the network as a preventive measure to prevent an aggressive cyberattack from spreading to new nodes, i.e., $\Lambda = 0$. However, in the case of a not-so-dangerous cyberattack, a target could also decide to allow new nodes to connect to the network with a specific *New Nodes Rate* (Λ) rate to avoid self-lockdown,

e.g., during the cyberattack, new vessels are deployed to reinforce the fleet's capabilities. These new vessels integrate into the existing fleet's network. The *New Nodes Rate* Λ represents the rate at which these new vessels with their systems (nodes) are added, increasing the fleet's capacity while also introducing additional nodes that must be secured.

7 Analysis of the SERDUX-MARCIM model

The system's behavior under different scenarios is showcased, and its performance is scrutinized for its fidelity to reality through various tests conducted on the proposed model. In this context, this section introduces the initial data, which is followed by the analysis of SERDUX-MARCIM concerning its parameters. A test of stability is also performed, like a comparison of the system's behavior with the SEIRS and MalSEIRS models. Ultimately, to underscore the utility of this proposal, this section shows the application of SERDUX-MARCIM to various attack circumstances. All code and data used in these simulations are available for open consultation in the project repository at: https://github.com/diegocabuya/SERDUX-MARCIM.

7.1 Executing SERDUX-MARCIM model with typical conditions

We assumed a typical network initially composed of a *Total Population Size* $N = 71$ nodes with the following distribution of nodes per state: i) 60 nodes in state *Susceptible* (S) which are operating normally but are vulnerable, ii) 9 nodes in state *Exposed* (E), which had contact with nodes that were attacked, iii) 0 nodes in state *Recovered* R, iv) 2 nodes in state *Degraded* D, which are currently under attack, v) 0 nodes in state *Unavailable* U, and vi) 0 nodes in state *Destroyed* X.

The parameters for this experiment are defined in Table 11, which represent a typical network with the following features:

- It is kept stable without adding new nodes, i.e., *New Nodes Rate* $\Lambda = 0$.
- The actions unrelated to the cyberattack making nodes unavailable are deficient, i.e., $\mu = 0.001$.
- The network has different security controls in different categories like *Corrective* (η), *Preventive* (υ), *Detective* (ζ), *Compensatory* (Ω), and *Deterrent* (α), all of them with an medium-low (MH) level of implementation, i.e. 0.5.
- In a correspondent way with the previous bullet, the *Impact Reduction Controls* and *Likelihood Reduction Controls* are 0.5.
- To simulate a low vulnerability of nodes to lose their immunity over time, $a = 0.2$ and $m = \frac{t_f}{8}$.

Table 11 Initial parameters for the execution of SERDUX-MARCIM

Symbol	Name	Value
Λ	New Nodes Rate	0
T_f	Simulation Time	35
a	Strength of the Cosine Damping	0.2
m	Length of the Cosine Period	$\frac{T_f}{8}$
β_0	Initial Propagation Rate	0.8
μ	Unavailability by Other Causes Rate	0.001
η	Corrective Controls	0.5
υ	Preventive Controls	0.5
ζ	Detective Controls	0.5
Ω	Compensatory Controls	0.5
α	Deterrent Controls	0.5
Γ	Impact Reduction Controls	0.5
ι	Likelihood Reduction Controls	0.5
Ψ	Cyberattack Degree	0.6
δ	Cyberattack Duration	0.6
L	Cyberattack likelihood	0.6

- The cyberattack affecting the network is highly dangerous, i.e., $\beta_0 = 0.8$, with a considerable *Cyberattack Degree* $\Psi = 0.6$, and *Cyberattack Duration* $\delta = 0.6$.

The simulation runs along 35 time units, which refers to the time scale that, depending on the context of the attack, can be hours, seconds, days, etc. After running SERDUX-MARCIM in Matlab, the behavior of the nodes is the one shown in Fig. 13. As expected, the population in states *Susceptible* (S), *Exposed* (E), and *Degraded* (D) approaches zero at the end of the simulation. Due to the initial conditions, more than half of the nodes moved to the state *Exposed* (E) before $t = 2$. As a result of the cyberattack, the number of nodes in state *Destroyed* (X) increased rapidly to 32 nodes (46% of the total). However, once there is an attack response from the cybersecurity team, the number of nodes in state *Resistant* (R) increases and stabilizes at 37 (53% of the total).

7.2 Analysis of the SERDUX-MARCIM model in terms of its parameters

This section analyzes the SERDUX-MARCIM model's behavior through a set of simulations that make dynamic adjustments to some of the parameters specified in Table 11 while maintaining others constant. These simulations were designed to cover a spectrum ranging from low to high values for each parameter.

Analyzing Fig. 14a, it sheds light on the impact of the *Cyberattack Duration* (δ), on the dynamics of the cyberattack. A low value ($\delta = 0.25$) does not significantly affect the network, as evidenced by the narrow width of the active

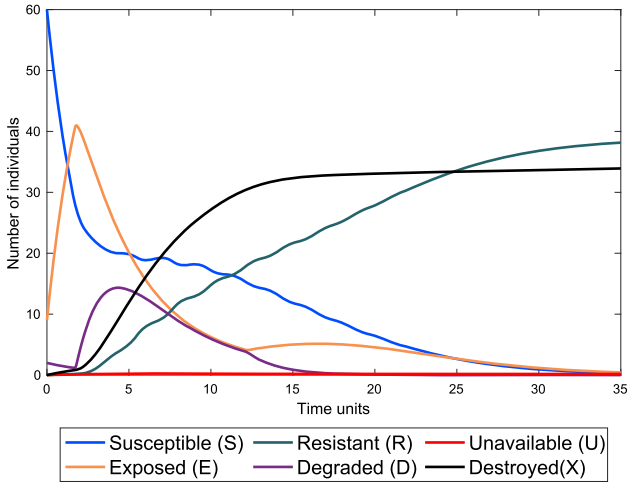


Fig. 13 Execution of SERDUX-MARCIM with typical conditions

interval of the *Cyberattack (Degraded)* rate(σ), which in this case is only $\Theta = \delta \cdot (1 - \Gamma) = 0.125$. In addition, such a short *Cyberattack Duration* (δ) fails to meet the criteria for *Cyberattack (Destroyed) Rate* (χ) due to $\delta < 0.5$, resulting in the absence of nodes in state *Destroyed* (X). In addition, with the gradual immunization efforts of the cybersecurity team, represented by a *Preventive Controls* implementation $\upsilon = 0.5$ and by an increasing *Sanitation Rate* ($\phi(t)$), the number of exposed nodes decreased over time. Conversely, when a high value for *Cyberattack Duration* (δ) is set, i.e., $\delta = 1$, which represents Highly Evasive Adaptive Threats (HEAT), a markedly different behavior is observed. In this last scenario, there is a notable peak at $t = 11$ with 25% of the nodes in state *Degraded* (D), 57% of the nodes in state *Destroyed* (X), and only 44% in state *Resistant* (R). This behavior contrast highlights the critical role of *Cyberattack Duration* (δ) in determining the severity and persistence of the cyber threat.

When varying the *Cyberattack Degree* (Ψ) it is possible to realize that for low values ($\Psi = 0.1$) there is not a significant impact on the network, which is evidenced in the absence of nodes in state *Unavailable* (U) and *Destroyed* (X) in Fig. 14b. A low value of Ψ also implies a low value in the *Cyberattack (Degraded) Rate* (σ), which justifies the substantial number of nodes in state *Exposed* (E) over the simulation time. In contrast, a high value of *Cyberattack Degree* (Ψ), $\Psi = 0.9$, leads to a notable increase in the number of nodes in state *Degraded* (D), with a peak of 17 nodes at $t = 4$, and a significant number of 39 nodes in state *Destroyed* (X) at $t = 35$. These findings highlight the significance of the *Cyberattack Degree* (Ψ) in the severity of cyber threats.

The *Cyberattack Likelihood* (L) influences the amount of nodes in state *Exposed* (E) as shown in Fig. 14c. Likewise, L also impacts ξ, which is the parameter in Eq. 22 used to control the speed of decaying of *Propagation Rate* (β), and there exists a positive correlation between these two variables. When L is low, e.g., $L = 0.1$, the target has some ability to resist the cyberattacks, in contrast when L is high, e.g., $L = 0.9$. That is why when $L = 0.1$, the number of nodes in state *Exposed* (E) is lower than when $L = 0.9$. It is also important to realize that when $L = 0.1$, even if the *Cyberattack Degree* (Ψ) is at a medium value of $\Psi = 0.5$, the harmonic mean function used to calculate ξ will be closer to the lowest one.

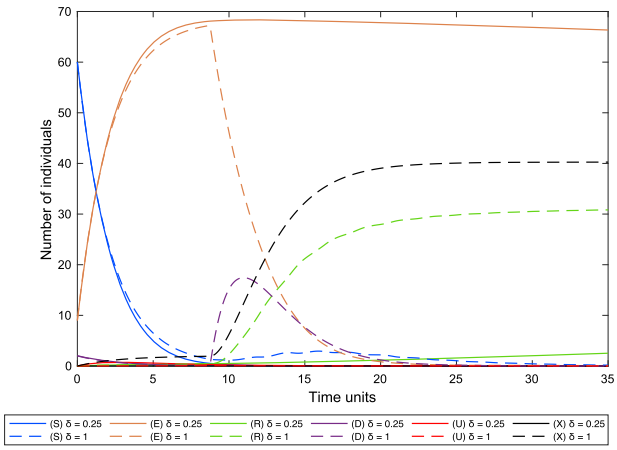
To validate the impact of adopting security controls focused on avoiding cyberattacks, the *Preventive Controls* (υ) was also varied. Increasing υ from 0.25 to 1 directly affected the network resilience. Specifically, a high value of υ, e.g., $\upsilon = 1$, correlated with a notable increase in the number of nodes in state *Resistant* (R), while simultaneously leading to a substantial decrease in nodes in states *Degraded* (D), *Unavailable* (U), and *Destroyed* (X), as indicated in Fig. 14f. This observation underscores the significance of implementing effective preventive measures to enhance network defenses and enhance recovery capabilities during cyberattacks.

Variations in the implementation of *Corrective Controls* (η) and *Detective Controls* (ζ) were also tested from 0.25 to 1, as shown in Fig. 14d and e. From these variations from a low to a high value, it is clear that strengthening corrective and detective countermeasures not only reduces the number of nodes in state *Exposed* (E) but also fewer nodes move to states *Degraded* (D) and *Destroyed* (X), which significantly enhances the network's resilience.

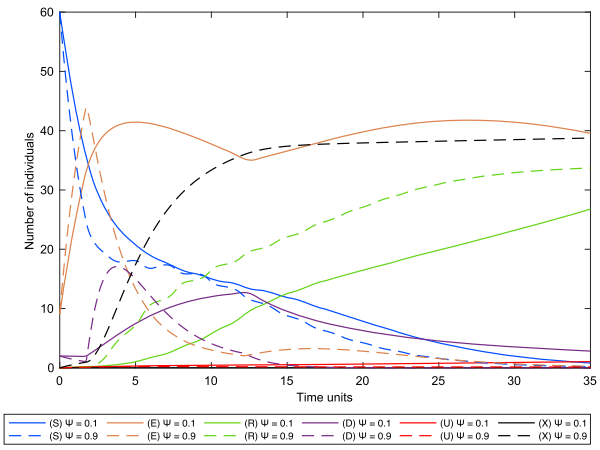
The previous analysis of parameters confirmed that the SERDUX-MARCIM model is coherent, and the best strategy for countering cyber threats and mitigating their potential adverse outcomes should be based on preventive controls. In other words, as soon as the level of *Preventive Controls* (υ) was in the highest value, the maximum number of nodes was recovered with a minimum level of destruction. This conclusion underscores that by taking proactive measures to mitigate threats before they materialize, organizations can effectively safeguard sensitive data and infrastructure organizations can effectively protect sensitive data and infrastructure.

7.3 Tests of stability of SERDUX-MARCIM model

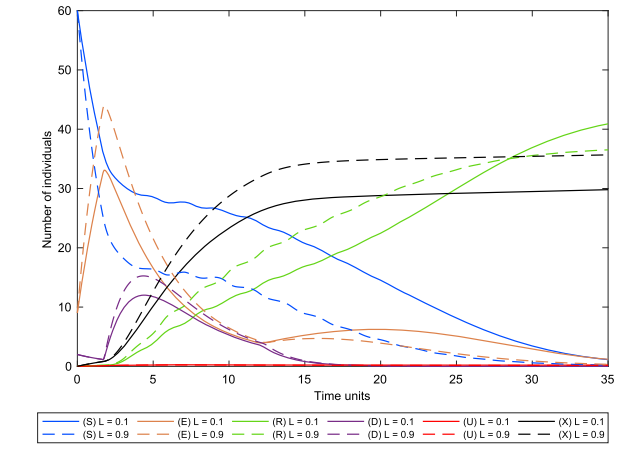
Assessing the stability of a system of differential equations requires its linearization, which is the process of selecting a fixed point and evaluating it in the resulting system of Jacobian matrix. This helps study a system's behavior under perturbations. Thus, the linearized system will be **stable** if every eigenvalue of the matrix is 0 or < 0. From this analysis, it can also be concluded that the original nonlinear system is also stable since a homeomorphism can be formed between the neighborhood of the fixed point and the linearized system.



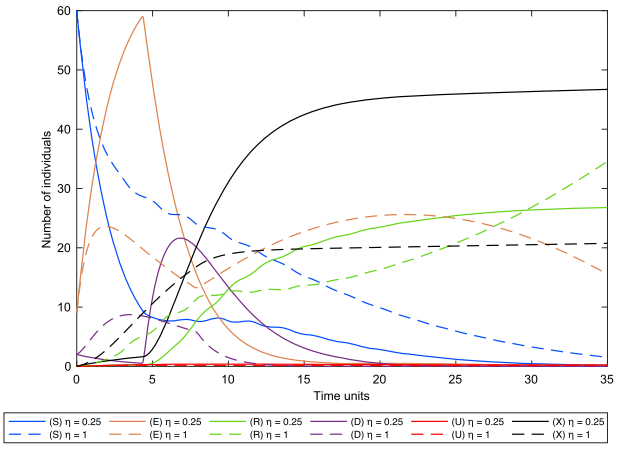
(a) Variation of the *Cyberattack Duration* (δ)



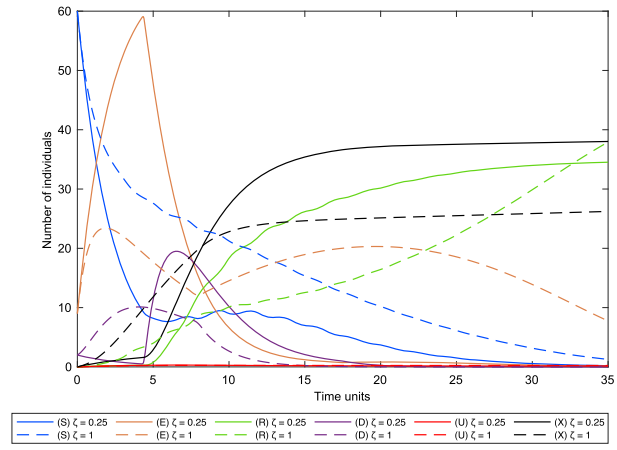
(b) Variation of the *Cyberattack Degree* (Ψ)



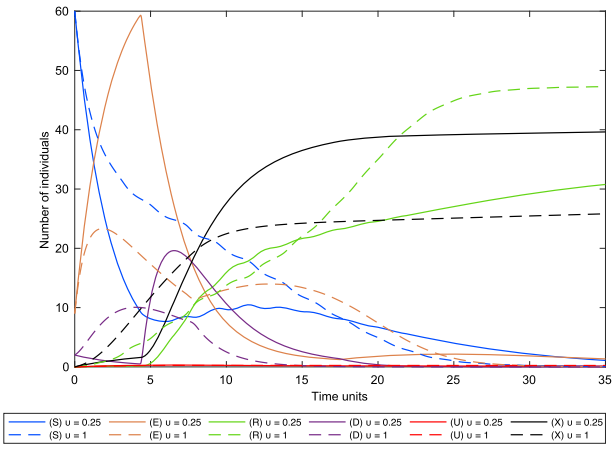
(c) Variation of the *Cyberattack Likelihood* (L)



(d) Variation of *Corrective Controls* (η) used in $\gamma(t)$



(e) Variation of the *Detective Controls* (ζ) used in ι



(f) Variation of *Preventive Controls* (υ) used in $\phi(t)$

Fig. 14 Simulation of the SERDUX model varying different constants and rates

Table 12 Parameters used in the tests of stability

Symbol	Name	Value
Λ	New Nodes Rate	0
a	Strength of the Cosine Damping	0.1
m	Length of the Cosine Period	120
β_0	Initial Propagation Rate	0.2
μ	Unavailability by Other Causes Rate	0.0001
η	Corrective Controls	0.1
υ	Preventive Controls	0.1
ζ	Detective Controls	0.25
Ω	Compensatory Controls	0.25
α	Deterrent Controls	0.25
Ψ	Cyberattack Degree	0.5
δ	Cyberattack Duration	0.9
L	Cyberattack Likelihood	0.75

However, because the proposed SERDUX-MARCIM model has a strong non-linear component and the states of nodes are sensitive to the initial conditions, the usual method of equilibrium points to state stability was inconclusive. Hence, two different alternative methods were used to validate the stability. The initial parameters used by such methods were established in Table 12.

7.3.1 Steady-state method

The first alternative method to validate the stability of the proposed model was the Steady-State method [54], which can be applied to nonlinear models. This method linearizes around a steady state, representing how the system output behaves as it approaches infinity. The premise is that the linearized model behaves similarly to the original nonlinear system when it remains close to equilibrium. The steady state is determined by selecting specific initial conditions that ensure the system remains stationary when simulating for a prolonged time. This implies that the system remains stable under small perturbations. When applying this method to SERDUX-MARCIM, it was found that the six eigenvalues of the Jacobian matrix are: -0.67, -0.42, -0.42, $3.6e-9$, -0.0021, and -0.0030. Each eigenvalue is negative, indicating that according to this method, the SERDUX-MARCIM system of differential equations is stable. Additionally, over time, it was observed that some eigenvalues approached zero but were never greater, indicating no potential instability.

7.3.2 Lyapunov exponents method

The method consists of taking two infinitesimally close initial conditions and finding the solution of the system for each one, thereby generating two trajectories. Then, it is determined how much the behavior changed between the two. If, with a slight alteration in the initial conditions, the trajectory differs from the original and does not get nearby, it can be said that it is unstable, while if the conditions are modified and the trajectory over time reduces or maintains its distance within the original trajectory, it can be said that it is stable. This is accomplished by measuring the growth speed of a distance between two points in a system, which is quantified using the Lyapunov exponent. In general, if every Lyapunov exponent is 0 or < 0, it can be concluded that the system is stable.

Table 13 Numerical results obtained by the Lyapunov Exponents method

Time	Maximal Exponent
1	1.569
100	0.042
200	0.019
500	0.007
1000	0.0034
2000	0.001614
3000	0.001001
5000	0.000508

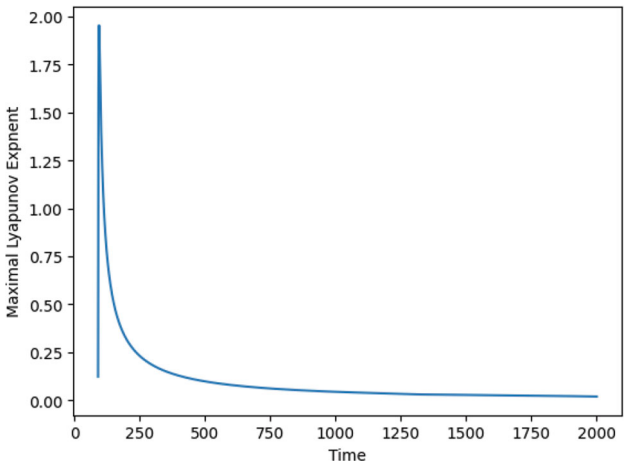


Fig. 15 Lyapunov Maximal Exponent

In the case of the SERDUX-MARCIM, empirical tests were performed due to the calculated exponents for the discretized numerical solution approximating the original system [55]. The observations showed that the longer the simulation time, the closer the calculated maximum Lyapunov exponent is to zero. The test was made with a population of 6200 nodes distributed in the states as 6045 susceptible, 124 exposed, and 31 degraded, establishing the values listed in Table 13, and graphed in Fig. 15.

The simulations show that the exponent decreases rapidly. The numerical method improves with a longer time and approaches the real value of the maximum exponent of this system is very close to zero, $\lambda = 0$. However, if the real value of the exponent is not zero, the results indicate that a very difference between them is negligible for practical purposes.

Table 14 Parameters for the comparative evaluation of SERDUX-MARCIM. Obs: α_1 is Unavailability by Other Causes Rate and α_2 is Deterrence Controls

Parameter	SERDUX-MARCIM	MalSEIRS	SEIRS
β_0 or β	0.8	0.8	0.8
Λ	0	0	0
c	–	1	–
γ	–	–	0.5
$\eta, \upsilon, \zeta, \Omega, \Gamma, \iota$	0.5	–	–
Ψ	0.6	–	–
δ	0.6	–	–
L	0.6	–	–
t_f	35	35	35
μ	0.001	0.001	0.001
α_1	–	0.3	0.3
α_2	0.5	–	–
σ	–	0.43	0.43
ω	–	–	0.1
a	0.1	0.1	–
m	1	1	–
ϕ	–	0.46	–
p	–	0	–
1- ξ4 or ξ	0.4	0.4	–

7.4 Comparative evaluation of SERDUX-MARCIM model

This section compares the SERDUX-MARCIM, SEIRS, and MalSEIRS models in an identical and typical cybersecurity scenario. Thus, all simulations considered the scenario and parameters defined in Sect. 7.1.The table 14 presents the specific parameter values used for each model in the simulations.

The results of the simulation for the SERDUX-MARCIM and SEIRS models are depicted in Figure. 16a, which unveils several insights into the capabilities of each model to simulate cyber threats and cyberattack propagation dynamics. Both models have conceptual differences; for example, the SEIRS model defines the 5 states (*Susceptible*, *Exposed*, *Infectious*, and *Recovered*), instead of the 6 states defined in SERDUX-MARCIM. In addition, the SEIRS model offers a simplistic portrayal of the spread of infectious disease as determined by Eq. 1, which uses constant transition rates unlike the SERDUX-MARCIM model.

Thus, several observations were obtained after analyzing the results presented in Fig. 16a. First, the SEIRS model exhibits a rapid initial recovery rate, surpassing that of the SERDUX-MARCIM model by a considerable margin, i.e., in just 5 time units, the number of recovered nodes in the SEIRS system is double of the resistant nodes in SERDUX-MARCIM. However, such behavior in the recovery rate is short-lived, as the number of recovered nodes in SEIRS declines steeply towards zero by $t = 35$. In contrast, the proposed model SERDUX-MARCIM demonstrated a more nuanced behavior, where the number of resistant nodes increases gradually and almost in a regular way, up to 54% of all nodes. This difference between the models is due to the SEIRS model's approach to simulating the cyberattack, where the *Machine Unavailability Rate caused by Malware* removes nodes from the system. In contrast, the SERDUX-MARCIM model is more resilient, accounting for the blue team's capabilities and allowing the system to recover more effectively from the attack.

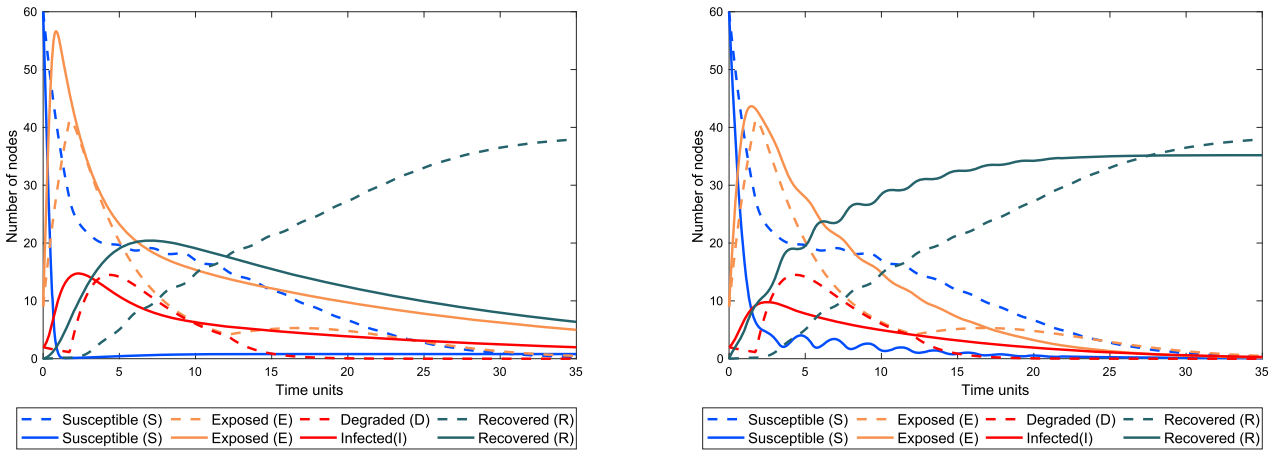
In addition, the SERDUX-MARCIM model initially exhibited a minor peak of infected nodes, i.e., nodes in state *Degraded* (D), but achieved 0 exposed nodes by $t = 16$. In contrast, the SEIRS model maintains an infection rate that decreases very slowly through the simulation. This is due to the SERDUX-MARCIM model considers the impact of reduction and corrective controls, which generate a decrease in the number of nodes in state *Degraded* (D).

Overall, these findings emphasize the proposed model's capacity to represent the impact of cyberattacks in different scenarios, thereby highlighting the importance of dynamic rates and adaptive security measures in combating evolving cyber threats.

To expand the comparative analysis, the results of comparing the MalSEIRS and SERDUX-MARCIM models are depicted in Fig. 16b. The MalSEIRS model is defined according to Eq. 3 and is an adaptation of the SEIRS model for generic cybersecurity scenarios, which considers time-dependent rates.

A closer examination of Fig. 16b reveals a critical distinction between SERDUX-MARCIM and MalSEIRS. In this sense, SERDUX-MARCIM evidences a higher number of nodes in state *Degraded* (D) state, than nodes in state *Infected* in MalSEIRS. This discrepancy is particularly pronounced at $t = 4$, with SERDUX demonstrating 50% more nodes than MalSEIRS. This is due to the modeling approach of MalSEIRS, in which the *Malware Execution Rate*(σ) is a constant, while in SERDUX-MARCIM the capabilities of the blue team are considered in the *Cyberattack (Degraded) Rate* $\sigma(t)$, which are calibrated at medium-low levels. Thus, SERDUX-MARCIM represents the prevailing conditions observed in real-world cybersecurity landscapes, where the cyber incident response capacities of the victim organization tackle cyberattack-induced degradation.

These discrepancies underscore the importance of considering the dynamics of attacker and target organizations as realistically as possible. This highlights the need for continuous refinement and enhancement of simulation models to ensure their effectiveness in simulating and analyzing cyber incidents, ultimately contributing to advancing cybersecurity research and practice.



(a) SERDUX-MARCIM (Dashed lines) vs SEIRS (Continuous lines)

(b) SERDUX-MARCIM (Dashed lines) vs MalSEIRS (Continuous lines)

Fig. 16 Comparison between SEIRS, MalSEIRS, and SERDUX-MARCIM

8 Applying SERDUX-MARCIM in a real cyberattack

This section describes the implementation of the proposed SERDUX-MARCIM model in a real cyberattack that targeted the maritime company Maersk in 2017. Such a cyberattack scenario was selected because of its relevance to the maritime sector as a crisis originating from a cybersecurity incident. The cyberattack scenario defined in this section was based on information gathered from: "Cyberattack: The Maersk Global Supply-Chain Meltdown" [56], "Understanding Leadership Competencies in Cyber Crisis Management: Insights from the Maersk Global Supply Chain Meltdown" [57], "SandWorm: A new era of cyberwar and the hunt for the Kremlim's most dangerous hackers" [58], "Implementing the Lessons Learned From a Major Cyberattack" [59], "Advanced Petya Ransomware and Mitigation Strategies" [60], and the official Maersk web site [61]. In addition, when some aspects of the cyberattack scenario were not found in literacy, these were inferred or interpreted for academic purposes.

The Maersk case was selected as the primary use case for validating the SERDUX-MARCIM model due to its prominence as one of the most representative cyberattacks in the maritime sector. This case provided a robust foundation for simulation, supported by extensive scientific documentation detailing the attack and its impact on maritime operations. Although the NotPetya cyberattack primarily targeted shore facilities, its cascading effects on vessel operations, such as the disruption of cargo handling and shore-to-ship communications, highlight the interconnected nature of maritime infrastructures. This case illustrates the model's capability to address shore-based scenarios while emphasizing its adaptability for broader applications, including vessel systems, when conceptualized within the model's flexible framework.

Under this context, an *Event n* refers to a milestone within the scenario evolution. An *Event n* can be into one of the typical 3 stages of a cyber crisis scenario [62]: pre-crisis, crisis, and post-crisis. For each *Event n*, it is possible to analyze the scenario from 3 perspectives: i) network situation, ii) level of services, and iii) level of cyber risk. In this case, executing the SERDUX-MARCIM model in the Maersk cyberattack included 5 events along the crisis stages, as shown in Fig. 17. Simulation 1 groups *Event 1* (Cyber Incident). Simulation 2 groups *Event 2* (Declaration of Crisis). Simulation 3 groups *Event 3* (Crisis) and *Event 4* (Post-crisis). Similarly, 3 simulations were executed to group these 5 events.

Use case scenario details and remarks are detailed in Tables 20 and 21 in the Appendix.

8.1 SERDUX-MARCIM simulation setup

For the application of SERDUX-MARCIM in the Maersk cyberattack case, it was considered the number of servers that Maersk had at the moment of the cyberattack to control his entire operation, i.e., *Total Population Size* $N = 6200$. In this scenario, 1 step of simulation time corresponds to 1 minute, and every simulation lasts 120 minutes. The variables and parameters used to run each simulation are shown in Table 15

Variables associated with the target, i.e., *Target Security Controls* (TSC), *Target Cyberintelligence Capability* (TCI), *Target Cyberdefense Capability* (TCD), and *Target Support and Sustainability Capability* (TSS), were evaluated between "Low" and "Medium Low" because Maersk, along with other shipping and supply industries, was considered in

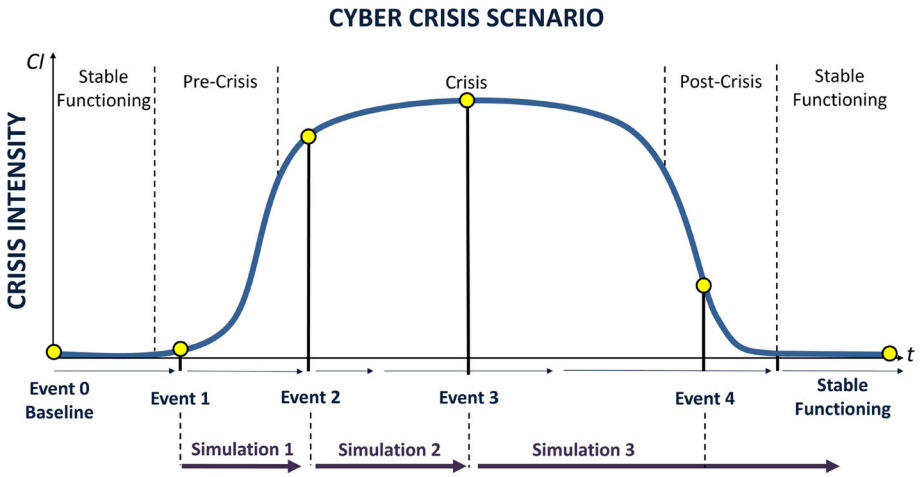


Fig. 17 Simulations and events defined for the application of SERDUX-MARCIM model in the Maersk cyberattack case of 2017

Table 15 Variables setup for the application of SERDUX-MARCIM model in the Maersk cyberattack case of 2017

Simulation			1	2	3
Variable		Sym	Event		
			1	2	3-4
Target Security Controls *(TSC)*	**Compensatory Controls**	Ω		0.25	
	Deterrence Controls	α		0.25	
	Detective Controls	ζ		0.25	
	Preventive Controls	υ	0.1		0.25
	Corrective Controls	η	0.1		0.25
Target Cyberintelligence Capability		TCI		0.25	
Target Cyberdefense Capability		TCD		0.1	
Target Support and Sustainability Capability		TSS		0.25	
Attacker Factors		ATF		0.75	
Vulnerability Factors		VUF		0.8	
Cyberattack Degree		Ψ		0.75	
Cyberattack Duration		δ	0.75		0.25
Parameters to control variables weight in *TCD*		d_n		0.25	
Parameter to control λ in L		l		0.1	
Parameters to control variables weight in λ		w_n		0.25	
Number of Node Connections		nl		3	
Parameter to control Γ in I		i		0.1	
Initial Propagation Rate		$\beta_{(0)}$		0.75	
Unavailability by Other Causes Rate		μ	0.0025	1	0.0025
New Nodes Rate		Λ		0	
Strength of the Cosine Damping in ω		a		0.1	
Length of the Cosine Period in ω		m		120	
Final Simulation Time in σ		tf		240	

2017 to be at a relatively low level of maturity compared with other sectors [59].

Attacker Factors (ATF) and *Vulnerability Factors* (VUF) were evaluated as "Medium High" because the attacker has high skills, geopolitical, and reward motives, and Maersk has a high likelihood that his vulnerabilities will be discovered and exploited. Thus, the attacker can identify and exploit Maersk's vulnerability.

It was known that the cyberattack was powerful and had the characteristics of ransomware; therefore, the cyber effect considered was "Denied", and consequently, *Cyberattack Degree* (Ψ), *Cyberattack Duration* (δ) and *Initial Propagation Rate* ($\beta_{(0)}$) were evaluated in "Medium High".

Parameters to control variables weight in *Target Cyberdefense Capability* (d_n) and parameters to control variables weight in *Target Likelihood* (w_n) were evaluated at 0.25

because they were considered to have the same weight. Parameter to control Target Likelihood in *Cyberattack Likelihood* (l) and parameter to control Impact Reduction Controls in *Cyberattack Impact* (i) were evaluated in 0.1 because it was considered that *Target Likelihood* (λ) and *Impact Reduction Controls* (Γ) had a low influence on the risk assessment, considering the maturity level of Maersk and the characteristics of the Cyberattack. The *Number of node connections* (nl) was evaluated in "Low", showing a basic level of interconnection between the 6200 servers.

The *Unavailability by Other Causes Rate* (μ) took the typical value 0.0025, meaning that at least 1% of the nodes in the states *Susceptible* (S), *Exposed* (E), *Degraded* (D), or *Resistant* (R) could change to state *Unavailable* (U), due to causes other than cyberattack. No new nodes were considered to be included during the simulations; for that reason, *New Nodes Rate* (Λ) is 0. The parameter *Strength of the Cosine Damping* (a) took a minimum value to reduce the stabilization speed of *Loss of Resistant Rate* (ω) to 0, and *Length of the Cosine Period m* took a value of 120 to adjust the length of the cosine period in ω to the total number of time (steps) considered in each scenario simulation.

Additionally, the parameter *Final Simulation Time in Cyberattack (Degraded) Rate* (tf) took a value of 240 in every simulation, which is twice the total number of time (steps) considered for every scenario simulation. This is because a complete cycle of *Cyberattack (Degraded) Rate* (σ) is completed in tf time (steps); thus, one complete cycle was established between simulations 1 and 2, and a new cycle began in simulation 3, taking into account the crisis evolution and remarks.

Finally, Fig. 18 shows the graphic evolution through the simulations regarding *Node States*, *Level of Services*, and *Rates*.

8.2 Results of simulation 1

The scenario of stable functioning where all the Maersk's services are working normally is represented from *Event 0* (Baseline) to some moments before *Event 1* (Pre-Crisis), as shown in Fig. 17. Simulation 1 starts with the occurrence of the cyber incident at *Event 1* (Pre-Crisis) and ends when the crisis starts at *Event 2* (Declaration of Crisis). Thus, the simulation results show that at *Event 1* (Pre-Crisis), 97.5% of the *Total Population Size* (N) moves to the state *Susceptible* (S), 2% move beyond to the state *Exposed* (E), and 0.5% move to state *Destroyed* (X). At the end of the simulation 1, i.e. at *Event 2* (Declaration of Crisis), 21.8% of the *Total Population Size* (N) remains in state *Susceptible* (S), and 0.1% in state *Exposed* (E). Additionally, 19% move to state *Resistant* (R), 0.1% to state *Degraded* (D), 0.2% to state *Unavailable* (U), and 58.8% to state *Destroyed* (X).

Table 16 Simulation results for the application of SERDUX-MARCIM model in the Maersk cyberattack case of 2017

Simulation	-	1		3	
			2		
Event	0	1	2	3	4
S	6200	6045	1354	0	106
E	0	124	2	0	60
R	0	0	1181	121	5542
D	0	31	3	0	0
U	0	0	15	2434	492
X	0	0	3645	3645	0
N	6200				
SER	6200	6129	2537	121	5708
Active Services	100 %	99.5 %	40.9 %	2 %	92 %
DUX	0	31	3663	6079	492
Inactive Services	0 %	0.5 %	59.1 %	98 %	8 %
Cyberattack Effect	Destroyed			Denied	
Cyber Risk Attack Severity (R)	Critical	High			
Cyberattack Likelihood (L)	High (0.75)				
Cyberattack Impact (I)	High (0.74)	Medium (0.49)			

The simulation 1 results are summarized in Table 16 and depicted in Fig. 18. In Fig. 18, it is possible to realize (a) the behavior of nodes in every state ($SERDUX$) during time; (b) the level of services during the time in terms of *Active* (SER) and *Inactive* (DUX) nodes; and (c) the transition rates behavior.

The simulation starts with 99.5% of active services and just 0.5% of inactive services. During the Simulation 1 the number of nodes in state *Susceptible* (S) decreased from 6045 to 1354. Nodes in state *Exposed* (E) initially increased, however, it was dramatically reduced between $t = 90$ and $t = 100$, due to the activation point of *Cyberattack (Degraded) Rate* (σ) and *Cyberattack Destroyed Rate* (χ), finally reaching a value of 2. The consequence of this situation is a cross effect between active (nodes in states SER) and inactive services (nodes in states DUX), which caused inactive services to exceed 50% and reach 59.1% at the end of the simulation.

Due to the "Destroyed" cyber effect, nodes in states *Susceptible* (S), *Exposed* (E), and *Degraded* (D) turn into state *Destroyed* (X), which is seen mainly in the behavior of these states between $t = 90$ and $t = 100$.

Although *Loss of Resistant Rate* (ω) decays during simulation 1, *Recovery Rate* (γ) and *Sanitation Rate* (ϕ) lightly increased between $t = 80$ and $t = 120$ with a minimum value, generating an effect in the network that increased the number of nodes in state *Resistant* (R) at the end of

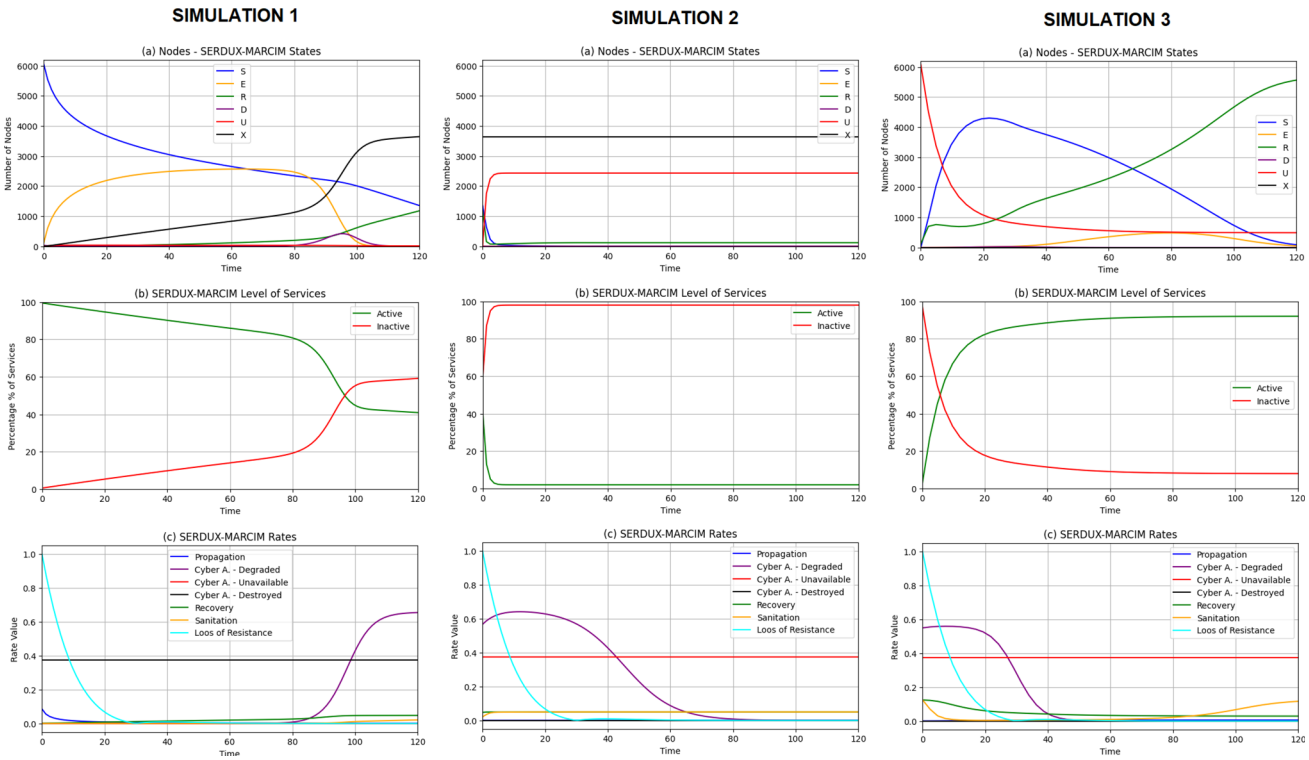


Fig. 18 Simulations results for the application of SERDUX-MARCIM model in the Maersk cyberattack case of 2017

simulation 1. This reflects Maersk's actions to contain the cyberattack and to maintain the primary services.

At the end of the simulation 1, i.e. at *Event 2* (Declaration of Crisis), the active service decreased to 40.9% (2537 nodes), and the inactive services increased to 59.1% (3663 nodes). These values are close to what Andy Powell mentioned in an interview in 2020 [59]: "The impact on servers was that 3500 out of 6200 servers were destroyed. Again, they could not be restored from backup due to reinfection".

Finally, the overall assessment of the *Cyber Risk Attack Severity* is "Critical" due to the *Cyberattack Likelihood* and *Cyberattack Impact* being valued as "High".

8.3 Results of simulation 2

The simulation 2 starts with the *Event 2* (Declaration of Crisis), which is the beginning of the crisis where the level of services is critical due to the ongoing cyberattack, and Maersk's IT team disconnected its global network, which took two hours since the cyber incident.

Simulation 2 ends with the *Event 3* (Post-Crisis), where almost the entire network (98%) turned *Inactive*; 2% of N moves to the state *Resistant* (R), 39.25% of N moves to the state *Unavailable* (U), and 58.75% of N moves beyond to the state *Destroyed* (D). Simulation 2 results are summarized in Table 16 and depicted in Fig. 18.

The simulation starts with 40.9% of active services and 59.1% of inactive services. The number of nodes in states *Susceptible* (S), *Exposed* (E) and *Degraded* (D) decreased to 0. Nodes in state *Resistant* (R) decreased from 1181 to 121. Nodes in state *Destroyed* (X) remained the same, and nodes in state *Unavailable* (U) increased dramatically from 15 to 2434. This behavior of the nodes is because Maersk's IT team disconnected its global network. Thus, *Unavailability by Other Causes Rate* (μ) took a value of 1 to reflect this decision in the simulation. The consequence of this situation is the polarization effect between active (nodes in states SER) and inactive services (nodes in states DUX), which causes inactive services to reach 98% at the end of the simulation.

Due to the effect of μ over the network, nodes in states *Susceptible* (S), *Exposed* (E) and *Degraded* (D) turn into state *Unavailable* (U), which is seen mainly in the behavior of these states between $t = 0$ and $t = 5$ of Fig. 18 (Simulation 2, a).

Although *Loss of Resistant Rate* (ω) decays during simulation 2, *Recovery Rate* (γ) and *Sanitation Rate* (ϕ) lightly increased between $t = 0$ and $t = 5$ with a minimum value, which allowed maintaining a few numbers of nodes in state *Resistant* (R) at the end of simulation 2. These nodes in state *Resistant* (R) correspond in the scenario to the Maersk's nodes located in Ghana, which had not been reached and had the only Domain Controller server not compromised; so the data from such a clean server were used to recover other Domain Controller servers.

At the end of the simulation 2, i.e. at *Event 3* (Post-Crisis), the active service decreased dramatically to 2% (121 nodes),

and the inactive services increased to 98% (6079 nodes). These values are close to what is mentioned in some documents of the case [56] [57] related to the decision Maersk's IT team disconnected its global network and the remaining network not compromised located in Ghana.

Finally, the overall assessment of the *Cyber Risk Attack Severity* is "High" due to the *Cyberattack Likelihood* being valued as "High", and *Cyberattack Impact* as "Medium".

8.4 Results of simulation 3

The simulation 3 starts with the *Event 3* (Crisis), which is the peak of the crisis, and the services are unavailable due to the ongoing cyberattack and the decision of Maersk to disconnect the global network, and almost the entire network is *Inactive*, 98% of N. This simulation ends with the *Event 4* (Pos-Crisis), when Maersk started actions to de-escalate the crisis to finally recover its stable functioning state. In this sense, Maersk used a Domain Controller Server in Ghana, which was not compromised, to initiate the restoration of services and the erradication of the cyberattack.

When starting the simulation at *Event 3* (Crisis), all nodes in *Destroyed* (X) state were considered unavailable, reaching a total of 6079 nodes in state *Unavailable* (U). Additionally, *Unavailability by Other Causes Rate* (μ) returned to a typical value of 0.0025. Simulation 3 results are summarized in Table 16 and depicted in Fig. 18.

Maersk improved its security controls to eradicate the cyberattack through the implementing of effective *Preventive Controls* (υ) and *Corrective Controls* (η); thus, at the end of the simulation, i.e. at *Event 4* (Pos-Crisis), the number of nodes in state *Destroyed* (X) decreased from 3645 to 0. The number of nodes in state *Resistant* (R) increased from 121 to 5542. The result of this situation is a cross-effect between active (nodes in states SER) and inactive services (nodes in states DUX), which caused inactive services to decrease to 8% and active services to reach 92% at the end of the simulation.

The *Recovery Rate* (γ) and *Sanitation Rate* (ϕ) positively affected the network, causing a significant number of nodes to state *Resistant* (R) during the simulation. Consequently, nodes in the *Unavailable* (U) state decreased rapidly between time $t = 0$ and $t = 40$. Nodes in *Susceptible* (S) state demonstrate the typical behavior of the effect of two actions taken simultaneously: node restoration and cyberattack eradication. In this sense, nodes in state *Unavailable* (U) transit to *Susceptible* (S) in the first stage of the security controls application. In the following stages, all nodes, including nodes in state *Susceptible* (S), turned into state *Resistant* (R). Finally, *Cyberattack Unavailable Rate* (∇), *Cyberattack Degraded Rate* (σ), and *Loss of Resistant Rate* (ω) had no significant effect on the nodes due to the established conditions.

At the end of the simulation 3, the active service increased to 92% (5708 nodes), and inactive services decreased to 8% (492 nodes). However, the consequences of cyberattack remain and it takes months to successfully eradicate the cyberattack [56] [57]. Taking this into account, at the end of the simulation 3, some nodes remained in states *Susceptible* (S), *Exposed* (E) and *Unavailable* (U).

Finally, the overall assessment of the *Cyber Risk Attack Severity* is "High" due to the *Cyberattack Likelihood* being valued as "High", and *Cyberattack Impact* as "Medium".

8.5 Netlogo implementation of SERDUX-MARCIM model

A NetLogo implementation of SERDUX-MARCIM model has been contributed. It can be used for experimenting and monitoring network and node outcomes. Also, Netlogo code and data used for the 3 simulations of the Maersk cyberattack of 2017 that were exposed in this section are available for open consultation in the project repository at https://github.com/diegocabuya/SERDUX-MARCIM. The graphical interface includes controls to set up and run simulations from scratch or run simulations using pre-load variables, which are used as inputs in the next simulation. The graphical interface of the implementation of the model in Netlogo is seen in Fig. 19. The interface is divided into 5 sections:

- A configuration section composed of sliders to set the variables' values established by the experimenter, i.e., *Total Population Size* (N), number of nodes per state *Susceptible* (S), *Exposed* (E), *Degraded* (D), *Unavailable* (U), parameters of the system of differential equations, Target, Cyberattack, and Attacker.
- A cyber risk section to view and control the values related to the cyber risk, i.e., *Cyber Risk Attack Severity* (R), *Cyberattack Likelihood* (L), *Cyberattack Impact* (I), *Cyberattack Degree* (Ψ), and *Cyberattack Duration* (δ).
- A section to visualize the network situation regarding the number of nodes in each state, i.e., Network status, and the active and inactive services, i.e., Level of Services.
- A section to control and visualize the transition rates associated with the system of differential equations.
- A section to visualize a network graph, with distinctive colors used for nodes depending on their state and connections with other nodes. Through this section, is also possible to point to a specific node to verify its properties.

9 Conclusions and future work

In this paper, we have developed SERDUX-MARCIM, a novel model that includes an adaptation of compartmental

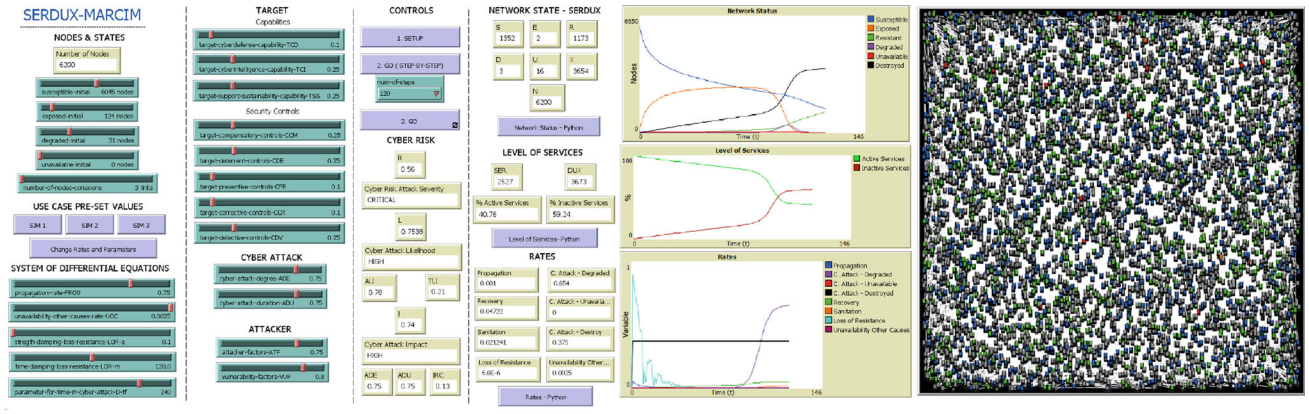


Fig. 19 Netlogo interface with the implementation of SERDUX-MARCIM model

models in epidemiology to cybersecurity and cyberdefense, to analyze and forecast the propagation of a cyberattack over maritime infrastructure. SERDUX-MARCIM considers network specific characteristics, target capabilities, attacker capabilities, and cyberattack characteristics as part of a holistic view of a cyberattack scenario. The construction of the model involved careful review and rigorous adjustment of variables, as well as alignment with widely recognized principles and frameworks in the field of cybersecurity.

Cyber Situational Awareness (CSA) is an important element in both cybersecurity and cyberdefence to inform processes and activities on the strategic, tactical, and operational levels. SERDUX-MARCIM is a proposal that belongs to the strategic level of CSA, which allows naval executive officers to make decisions, agnostic of protocols and underlying technologies, in scenarios of cyberattacks over maritime infrastructure.

The proposed model was effectively tested and demonstrated its capability to simulate crises in maritime environments from two perspectives: stability and performance, as outlined in Sect. 7, and its application in a real-case scenario to demonstrate its effectiveness, as discussed in Sect. 8. Including time-dependent rates allows us to model the transitions of nodes between states, thereby improving our understanding of changes occurring during a cyber crisis. These properties of SERDUX-MARCIM support strategic decision-making and provide a robust framework to address cybersecurity challenges in maritime settings.

Our proposal represents an important contribution to the decision-making process in a strategic layer, which considers the status information of each computational node. However, important technical information coming from other layers, like operational and tactical, may enrich the process and tackle restrictions that a single-layer perspective faces, like a strategic layer.

The SERDUX-MARCIM model was validated through a real-world case study, specifically the NotPetya ransomware attack on Maersk in 2017. Using actual data and scenarios from the available literature, this case study demonstrated the model's applicability in simulating and analyzing cyberattack propagation in a maritime context, addressing critical challenges in maritime cybersecurity, and reflecting the dynamics of a real cyberattack. Based on the results, we conclude that effective mitigation of cyberattacks requires balancing cybersecurity and cyberdefense capacities. Additionally, a proper cyber risk assessment should identify, analyze, and evaluate potential cybersecurity threats; however, it should also consider the organization's risk level, to develop appropriate strategies that reduce the impact and severity of a cyberattack. The validation of SERDUX-MARCIM in a real scenario also demonstrated limited access to well-documented cyberattacks, highlighting the need for greater collaborative efforts among various stakeholders to promote knowledge sharing and raise awareness. Comprehensive documentation fosters awareness and facilitates the development of practical solutions to address the threats in a better way. As future validations, we plan to develop a wargame simulator to enable strategic-level experimenters to test hypotheses and evaluate courses of action in realistic scenarios. Additionally, the model is intended to be applied in an operational setting, such as a Naval Cyber Command, to assess its effectiveness in a live environment. These initiatives aim to further validate the model and demonstrate its practical utility.

In future works, we aim to enhance the proposed model by developing an agent-based mathematical modeling approach, including an updated Netlogo implementation. This allows us to capture individual-level behaviors and interactions to better understand system dynamics. In addition, we plan to incorporate a new time-dependent dynamic cyber risk approach to assess and mitigate evolving cyber threats in

real-time in an adaptive way. Future opportunities to improve SERDUX-MARCIM can be extended to other organizational environments without the loss of expressiveness.

Future research will involve testing the robustness of the proposed SERDUX-MARCIM model under various cyberattack scenarios. By adjusting key parameters, such as the severity, speed, and method of propagation of cyberattacks, we aim to analyze the model's adaptability to different types of threats and assess its performance under diverse conditions.

Another line of investigation will focus on evaluating SERDUX-MARCIM during complex, multi-phase cyberattacks. These simulations involve scenarios where attackers modify their behavior over time, transitioning through different stages of the cyberattack. The goal is to understand how the model reacts to dynamic threats and its capacity to anticipate or respond to shifts in attack strategies.

Given that cyberattacks often affect both military and civilian infrastructures, future work will assess the applicability of SERDUX-MARCIM in hybrid environments. This includes testing the model's effectiveness in scenarios where military operations intersect with civilian systems, such as shared communication networks or critical infrastructure, to ensure comprehensive defense strategies.

Finally, a key future initiative is to engage cybersecurity and cyberdefense experts in the evaluation of the proposed SERDUX-MARCIM model via wargaming exercises. This interactive approach allows experts to explore the model in a user-friendly environment, providing valuable feedback to further refine its usability and applicability in real-world cyberdefense contexts.

Appendix A Tables

Table 17 Reference conditions for node's transitions between states

From	To	Situation motivating the transition
S	*E*	When a susceptible node had contacted with an attacked node in any of its states (Degraded, Unavailable, Destroyed) and may also be compromised, despite it does not show symptoms
	R	When a node gets the cybersecurity countermeasures that make it immune against a specific threat
	U	When a node becomes in a fully inoperative state by causes other than cyberattack in progress, including the decision of the node administrator
E	*D*	When the cyberattack had executed its functionality over the node generating a disrupted or degraded cyberattack effect on the node
	R	When a node gets the cybersecurity countermeasures that make it immune against a specific threat
	U	When a node becomes in a fully inoperative state by causes other than cyberattack in progress, including the decision of the node administrator
R	*S*	When a node has lost its immunity due to the cyberattack mutation or changes in the target's capabilities
	U	When a node becomes in a fully inoperative state by causes other than cyberattack inpr ogress, including the decision of the node administrator
D	*R*	When a node gets the cybersecurity countermeasures that make it immune against a specific threat
	U	When the cyberattack had executed its functionality over the node generating a denied cyberattack effect on the node
		When a node becomes in a fully inoperative state by causes other than cyberattack in progress, including the decision of the node administrator
	X	When the cyberattack had executed its functionality over the node, generating a destroyed cyberattack effect on the node
U	*R*	When a node gets the cybersecurity countermeasures that make it immune against a specific threat
	X	When the cyberattack had executed its functionality over the node, generating a destroyed cyberattack effect on the node
X	-	None

Table 18 SERDUX-MARCIM variables and assessment - Part 1 (Target)

VARIABLE		SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED	**MAIN**			**(Low - 0.25) (Medium Low - 0.5) (Medium High - 0.75) (High - 1)**	
***Target Security Controls* (*TSC*)**	*Compensatory Controls*	Ω	What is the implementation level of physical, technical, and administrative measures to reduce the risk of an existing or potential control weakness resulting in errors or omissions?	(L) - Insufficient:Very few measures are carried out (ML) - Basic: Minimum measures are carried out.	(MH) - Mature: Most of the measures are carried out (H) - Optimized: All required measures are carried out
	Deterrence Controls	α	What is the implementation level of physical, technical, and administrative measures to generate warnings that can prevent potential risks?	(L) - Insufficient:Very few measures are carried out (ML) - Basic: Minimum measures are carried out.	(MH) - Mature: Most of the measures are carried out (H) - Optimized: All required measures are carried out
	Detective Controls	ζ	What is the implementation level of physical, technical, and administrative measures to warn about violations or attempted violations of the security policy?	(L) - Insufficient:Very few measures are carried out (ML) - Basic: Minimum measures are carried out.	(MH) - Mature: Most of the measures are carried out (H) - Optimized: All required measures are carried out
	Preventive Controls	υ	What is the implementation level of physical, technical, and administrative measures to inhibit attempted security policy violations?	(L) - Insufficient:Very few measures are carried out (ML) - Basic: Minimum measures are carried out.	(MH) - Mature: Most of the measures are carried out (H) - Optimized: All required measures are carried out
	Corrective Controls	η	What is the implementation level of physical,technical, and administrative measures to remedy the impact of an attack?	(L) - Insufficient:Very few measures are carried out (ML) - Basic: Minimum measures are carried out.	(MH) - Mature: Most of the measures are carried out (H) - Optimized: All required measures are carried out
***Target Cyberintelligence Capability* (*TCI*)**	*Threat Identification and Analysis*	*TIA*	How easily can the organization effectively discover, identify, and analyze cybersecurity threats and vulnerabilities?	(L) - Practically impossible (ML) - Difficult	(MH) - Easy(H) - Automated tools available
	Information Sharing	*INS*	How effectively does the organization share relevant cybersecurity and cyberdefense information with appropriate partners?	(L) - Low effectiveness (ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness (H) - High effectiveness
	Security Operation Enhancement	*SOE*	How effectively does the organization feed, improve, and optimize cybersecurity operations through the use of intelligence-driven approaches and technologies?	(L) - Low effectiveness (ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness (H) - High effectiveness

Table 18 continued

VARIABLE		SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED	**MAIN**			**(Low - 0.25)**	**(Medium Low - 0.5) (Medium High - 0.75) (High - 1)**
	Cyber Awareness	*CYA*	How effectively does the organization promote awareness of cybersecurity and cyberdefense risks and best practices among its personnel?	(L) - Low effectiveness (ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness (H) - High effectiveness
	Digital Forensics and Malware Analysis	*FMA*	How easily can the organization effectively conduct digital forensics and analysis of cyber incidents?	(L) - Practically impossible (ML) - Difficult	(MH) - Easy (H) - Automated tools available
***Target Cyberdefense Capability* (*TCD*)**	*Active Defense*	*ACD*	What is the maturity level regarding People,Processes, and technology to take advanced defense measures on network, software,monitoring, and management against cyber threats?	(L) - Low maturity level (ML) - Medium-low maturity level	(MH) - Medium-high maturity level(H) - High maturity level
	Cyber Threat Intelligence and Hunting	*TIH*	What is the maturity level regarding People,Processes, and Technology to actively search,gather, and analyze information about actual and potential cyber threats and adversaries?	(L) - Low maturity level (ML) - Medium-low maturity level	(MH) - Medium-high maturity level(H) - High maturity level
	Cyberdeterrence	*CDT*	What is the maturity level regarding Capacity, Determination, and Declaration to influence an adversary's behavior and discourage them from engaging in unwanted or malicious activities in cyberspace?	(L) - Low maturity level (ML) - Medium-low maturity level	(MH) - Medium-high maturity level(H) - High maturity level
	Offensive	*OFF*	What is the maturity level regarding People,Processes, and Technology to conduct offensive cyber operations and cause cyberattack effects on targets?	(L) - Low maturity level (ML) - Medium-low maturity level	(MH) - Medium-high maturity level (H) - High maturity level

Table 18 continued

VARIABLE RELATED	MAIN	SYM	GENERAL MEANING OR QUESTION	ASSESSMENT (Low - 0.25)	(Medium Low - 0.5)	(Medium High - 0.75)	(High - 1)
Target Support and Sustainability Capability (***TSS***)	*Governance and Strategy*	*GOS*	How effectively does the organization establish rules, processes, procedures, and practices that guide it in managing and mitigating cybersecurity risks?	(L) - Low effectiveness	(ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness	(H) - High effectiveness
	Cooperation and Collaboration	*COC*	How effectively does the organization work with other entities and partners to actively address shared cyber threats and challenges?	(L) - Low effectiveness	(ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness	(H) - High effectiveness
	Laws, Regulations and Standards	*LRS*	How effectively does the organization comply with relevant laws, regulations, and standards in cybersecurity and cyberdefense practices?	(L) - Low effectiveness	(ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness	(H) - High effectiveness
	Science, Technology and Innovation	*STI*	What is the maturity level regarding People,Processes, and Technology to conduct science,technology, and innovation activities to improve cybersecurity and cyberdefense practices?	(L) - Low maturity level	(ML) - Medium-low maturity level	(MH) - Medium-high maturity level	(H) - High maturity level
	Education and Training	*EDT*	How effectively does the organization provide education and training in cybersecurity and cyberdefense to its personnel?	(L) - Low effectiveness	(ML) - Medium-low efectiveness	(MH) - Medium-high effectiveness	(H) - High effectiveness

Table 19 SERDUX-MARCIM variables and assessment - Part 2 (Attacker - Cyberattack - Cyber Risk - System of Differential Equations)

VARIABLE		SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED	**MAIN**			**(Low - 0.25) (Medium Low - 0.5) (Medium High - 0.75) (High - 1)**	
AttackerFactors(ATF)	*Skill Level*	*SKL*	How technically skilled is this group of threat agents?	(L) - Some technical skills (ML) - Advanced computer user	(MH) - Network and programming skills (H) - Security penetration skills
	Motive	*MOT*	How motivated is this group of threat agents to find and exploit this vulnerability?	(L) - No reward (ML) - Low reward	(MH) - Possible reward (H) - High reward
	Opportunity	*OPP*	What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability?	(L) - Full access or expensive resources required (ML) - Special access or resources required	(MH) - Some access or resources required (H) - No access or resources required
	Size	*SIZ*	How large is this group of threat agents?	(L) - Developers (ML) - System administrators or intranet users	(MH) - Partners or authenticated users (H) - Anonymous internet users
Vulnerability Factors(VUF)	*Ease of Discovery*	*EAD*	How easy is it for this group of threat agents to discover this vulnerability?	(L) - Practically impossible (ML) - Difficult	(MH) - Easy (H) - Automated tools available
	Ease of Exploit	*EAE*	How easy is it for this group of threat agents to actually exploit this vulnerability?	(L) - Theoretical (ML) - Difficult	(MH) - Easy (H) - Automated tools available
	Awareness	*AWA*	How well known is this vulnerability to this group of threat agents?	(L) - Unknow (ML) - Hidden	(MH) - Obvious (H) - Public Knowledge
	Intrution Detection	*IND*	How likely is an exploit to be detected?	(L) - Active detection in application (ML) - Logged and reviewed	(MH) - Logged without review (H) - Not logged

Table 19 continued

VARIABLE			SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED		**MAIN**			**(Low - 0.25) (Medium Low - 0.5) (Medium High - 0.75) (High - 1)**	
Cyber Attack Degree (Ψ)	*Technical Impact*(τ)	Loss of Confidentiality	*LCO*	How much data could be disclosed and how sensitive is it?	(L) - Minimal non-sensitive data disclosed (ML) - Minimal critical data disclosed	(MH) - Extensive critical data disclosed (H) - All data disclosed
		Loss of Integrity	*LIN*	How much data could be corrupted and how damaged is it?	(L) - Minimal slightly corrupt data (ML) - Minimal seriously corrupt data	(MH) - Extensive seriously corrupt data (H) - All data totally corrupt
		Loss of Availability	*LAV*	How much service could be lost and how vital is it?	(L) - Minimal secondary services interrupted (ML) - Minimal primary services interrupted	(MH) - Extensive primary services interrupted (H) - All services completely lost
		Loss of Accountability	*LAC*	Are the threat agents' actions traceable to an individual?	(L) - Fully traceable (ML) - Possibly traceable	(MH) - Partially anonymous (H) - Completely anonymous
	Business Impact (ρ)	*Financial Damage*	*FID*	How much financial damage will result from an exploit?	(L) - Minor effect on annual profit (ML) - Significant effect on annual profit	(MH) - High effect on annual profit (H) - Bankruptcy
		Reputational Damage	*RED*	Would an exploit result in reputation damage that would harm the business?	(L) - Minimal damage (ML) - Loss of major accounts	(MH) - Loss of goodwill (H) - Brand damage
		Non-Compliance	*NOC*	How much exposure does non-compliance introduce?	(L) - Minor violation (ML) - Notable violation	(MH) - Clear violation (H) - High profile Violation
		Privacy Violation	*PRV*	How much personally identifiable information could be disclosed?	(L) - One individual (ML) - Hundreds of people	(MH) - Thousands of people (H) - Millions of people
Cyberattack Duration			δ	How would you rate the duration of the cyberattack?	(L) - Short term (ML) - Temporary	(MH) - Persistent (H) - Permanent

Table 19 continued

VARIABLE		SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED	MAIN			(Low - 0.25) (Medium Low - 0.5) (Medium High - 0.75) (High - 1)	
Target Cyberdefense Capability (*TCD*)	*Parameters to control variables weight in TCD*	$d1\ d2\ d3\ d4$	How important is the variable (*ACD*, *TIH*, *CDT*, *OFF*) in the organizational context to calculate *TCD*? $\sum_{n=1}^{4} d_n = 1$	(L) - Low Importance (ML) - Medium-low importance	(MH) - Medium-high importance (H) - High importance
Cyberattack Likelihood L	*Parameter to control* λ *in L*	l	How much influence λ has in the reduction of L.? $l \in (0, 0.5)$	(L) - Low influence - 0.1 (ML) - Medium-low influence - 0.25	(MH) - Medium-high influence - 0.35 (H) - High influence - 0.5
Target Likelihood λ	*Parameters to control variables weight in* λ	$w1\ w2\ w3\ w4$	How important is the variable (ι, *TCI*, *TCD*, *TSS*) in the organizational context to calculate λ? $\sum_{n=1}^{4} w_n = 1$	(L) - Low Importance (ML) - Medium-low importance	(MH) - Medium-high importance (H) - High importance
Target's Network Traffic θ	*Number of node connections*	nl	How many connections, on average, have every node in the network? (Consider the Total Population Size N)	(L) - $N/2.5$ (ML) - $N/5$	(MH) - $N/7.5$ (H) - $\geq N/10$
Cyberattack Impact I	*Parameter to control* Γ *in I*	i	How much influence Γ has in the reduction of I.? $i \in (0, 0.5)$	(L) - Low influence - 0.1 (ML) - Medium-low influence - 0.25	(MH) - Medium-high influence - 0.35 (H) - High influence - 0.5
Simulation Time		T_f	How much will the total simulation time be (number of steps)?	Depends on the experimenter and scenario, $t_f > 0$	
Propagation Rate β	*InitialPropagation Rate*	$\beta_{(0)}$	What is the initial speed (propagation) at which the cyberattack spreads through network after its launch?	(L) - Low propagation (ML) - Medium low propagation	(MH) - Medium high propagation (H) - High propagation

Table 19 continued

VARIABLE		SYM	GENERAL MEANING OR QUESTION	ASSESSMENT	
RELATED	**MAIN**			**(Low - 0.25) (Medium Low - 0.5) (Medium High - 0.75) (High - 1)**	
Unavailability by Other Causes Rate		μ	What is the weight of the factors not directly related to a cyberattack that can cause nodes in states S, E, D, or R to enter the state U?	(L) - Low: $\mu <$ 0.0025 (ML) - Typical: $\mu = 0.0025$	(MH) - Medium: $0.0025 < \mu \leq 0.01$ (H) - High: $0.01 < \mu \leq 1$
New Nodes Rate		Λ	How many new nodes will be added to the target's network every time step t?	Depends on the experimenter and scenario, $\Lambda \geq 0$	
Loss of Resistance Rate ω	*Strength of the Cosine Damping*	a	How fast does ω stabilize at 0?	(L) - Very Slow: $a <$ 0.5 (ML) - Slow: $0.5 < a \leq 1$	(MH) - Fast: $1 < a \leq 10$ (H) - Very Fast: $a > 10$
	Length of the Cosine Period	m	How long does it take the oscillations of ω?	(L) - Too Short: $m < t_f/2$ (ML) - Short: $t_f/2 < m \leq t_f$	(MH) - Typical: $m = t_f$ (H) - Too Long: $m > t_f$
Cyberattack (Degraded) Rate σ	*FinalSimulation Timein* σ	tf	What is the final time for the simulation of ω complete behavior (initial and final phase)?	Typically t_f is equal to T_f (Total simulation time), however, it depends on the experimenter and scenario to evaluate the behavior of the initial and final phase functions in σ	

Table 20 Maersk cyberattack scenario details

ACTORS		
TARGET: Maersk	**ATTACKER: SandWorm**	**CYBERATTACK: NotPetya**
Møller - Maersk, in 2017, was a leading global shipping and logistics company that provides a wide range of transportation services. The company has a strong presence in container shipping, terminal operations, oil and gas exploration, and other related activities; Maersk's logistics solutions encompass the transportation of 12 million containers annually, delivering to every corner of the globe; For each container shipped, up to 30 parties may be involved. Maersk represented nearly 20% of the world's cargo shipping capacity (world trade), with 300 Tugs and 800 Vessels, 19,000 containers, operations in 343 ports and terminals globally, 574 offices in 130 countries around the globe, 6200 Servers and 150 Domain controller servers.	The attribution of NotPetya has been linked to a threat actor known as the SandWorm Team, which is believed to have ties to state-sponsored hackers. However, it's essential to note that attributing cyberattacks to specific actors or nations can be challenging due to the use of sophisticated techniques to conceal identities and the potential for false flags. The motivation behind SandWorm's NotPetya attacks against multiple organizations remains a subject of speculation. Some experts believe it was a politically motivated cyber operation intended to disrupt a specific nation's infrastructure. In contrast, others think it might have been a broader campaign that spiraled out of control.	NotPetya is a destructive malware that combines ransomware with the ability to propagate itself across a network to generate a disrupted effect over the computational systems. The attackers used leaked exploits of Microsoft Windows to develop cyberattacks, including EternalBlue and EternalRomance; EternalBlue allowed attackers to remotely access infected systems, while EternalRomance escalated the privilege to control or modify systems without detection. NotPetya also uses a credential harvester Mimikatz, to retrieve credentials from the system
General Scenario Description		
The scenario centers around the cyberattack that occurred against Maersk in 2017. Maersk, a major maritime services company, was hit by a cyberattack involving the NotPetya ransomware. Although the malware was initially aimed at Ukrainian businesses, it quickly spread and caused significant cyber effects on Maersk's operations worldwide for several days. Initially, ransomware encrypted files and demanded Bitcoin payments for decryption. However, the cyberattack evolved destructively, critically affecting the MAERSK level of services, highlighting the vulnerability of critical infrastructures and the need for improved cybersecurity measures in the maritime sector.		
CyberWar		
Since 2014, Ukraine has been the target of cyberattacks directed at its key economic and infrastructure components, which a state might have sponsored. In December 2015, compromised accounts delivered malware to the Ukrainian power grid, causing a widespread power blackout. The malware also wiped computer drives to delay restoration, and a coordinated DDoS attack disabled the power company's phone lines [63].		

Table 20 continued

ACTORS		
General Event Situation		
Baseline	2015 to June 27, 2017	Maersk initiated a digital transformation plan to enhance its processes and competitiveness in the years leading up to the cyberattack. In 2016, Maersk's senior system administrators warned the company that its network of over 80,000 computers was vulnerable to attack. Most of the company's services were interconnected and automated through cloud computing; however, most of these services were running on outdated operating systems. Maersk, along with other shipping and supply industries, was considered in 2017 to be at a relatively low level of maturity compared with other sectors. During the first semester of 2017, Maersk had a strong position in the market, and its mission-critical information services are operating normally worldwide.
Pre-Crisis	June 27, 2017. 10:00 am	Several Maersk workers stand around the help desk, each with a laptop, looking confused and uncertain. Some laptops display a message that says, "repairing file system on C:" with a warning that says, "not to shut down the computer." Other laptops show a more alarming message, "Oops, your important files are encrypted," and demand payment of $300 worth of Bitcoin to decrypt the files. The attack looks like ransomware or scammer, but the origin or scope of is unclear.
Crisis Declaration	June 27, 2017. 12:00 pm	A CRISIS is declared when risks that were never identified materialize or when a set of previously identified risks materialize simultaneously, provoking a situation that is not manageable with established continuity procedures. In the Maersk case, having a complete shutdown of the corporate computer network was a clear reason to declare a crisis. Maersk's global network was disconnected by its IT team in two hours. The Maersk Emergency Response Center in London is in charge of restoring global operations. Transparency about the current corporate situation with Maersk's level-C members allows the authorization to request collaboration with specialized cybersecurity organizations like Deloitte, which offered guidance to handle the crisis. Disruptions in critical Maersk operations (customer attendance, logistics, compliance, communications), due to the exploitation of multiple vulnerabilities in the operating systems that hold critical information systems, provoked by an attacker using a strategy with NotPetya.
Crisis	June 27, 2017. 2:00 pm	Maersk network was based on 150 Domain Controller Servers distributed around different Maersk branches. These servers were synchronized with each other, guaranteeing replication of these servers. The Maersk Emergency Response Centre in London worked a lot to find 1 Domain Controller server that the cyberattack had not reached, so the data from such a clean server was used to recover other Domain Controller servers. Such a rescuer server was found on the Maersk branch in Ghana.
Post-Crisis	10 days after Crisis	Operations are re-established, but fines and compensations must be addressed due to contractual breaches caused by the ransomware cyberattack. This is in addition to $300 million for expenses and lost earnings during the 10 days that took the recovery.

Table 21 Network status, level of services, materialized risk and impacts at each event of the Maersk cyberattack scenario

Event	0 Baseline	1 Pre-Crisis	2 Declaration of Crisis	3 Crisis	4 Pos-crisis
Simulation	–	1	2	3	
Time	2015 to June 27, 2017	June 27, 2017. 10:00 am	June 27, 2017. 12:00 pm	June 27, 2017. 2:00 pm	10 days after Crisis
Network	Normal Operation - Maersk's network comprises various technologies to optimize its operations and services.	Partial Affectation - Cyber Incident - All the PCs rebooted in Copenhagen, causing screens to turn black. - Delay to realize the issue. - Employees started to unplug their machines.	Total Affectation - Critical situation - Central servers (Domain controllers) are completely unavailable or destroyed. - Authenticating and retaining access to production servers and critical information systems aren't available. - Network services are seriously impacted, and basic services like internal connectivity, Internet, e-mail, file transfer, among others, aren't available.	Partial Affectation - Maersk implement the necessary security controls to de-escalate the crisis. - Essential network services are working again working.	
Level of Services	Normal Operation	Partial Affectation - Some services impacted - Communications servers are inoperable. - Maersk has problems to recover information and coordinate a response. - Fixed phones became inoperable. - There is no information about how many domain controllers are inoperative (partial o full). - The real level of services and scope were unclear.	Total Affectation - Main information systems are inaccessible. - The majority of services are not working, like the attention of customers, processing of incoming cargo, logistics of cargo ships on route, and the provision of data interfaces with local organizations.	Partial Affectation - Most critical information systems have been recovered and tested. - Due to manual operations, there are multiple inconsistencies due to data not being loaded into the systems.	
Materialized Risk	N/A	- Disruption in the headquarters and some administrative offices. - The status of operational and tactical services is unclear.	- Disruptions in critical Maersk operations.	- Operations are re-established.	
Operative Impact	N/A	- 10,000 employees with no possibility of doing their job. - No formal communications.	- 10,000 employees with no possibility of doing their job.	- Delays in operation. - Reprocessing of activities. - Data inconsistency.	
Legal Impact	N/A	- Not established yet	- Non-compliance with different Service Level Agreements (SLA) triggers different legal consequences.	- Multiple legal claims. - Investigations are in process by maritime authorities.	
Reputational Impact	N/A	- Not considered yet. - The focus was on determining the actual situation.	- Customer's distrust of their data security and cargo status. - Authorities distrust the security of operations at Maersk.	- Negative impact on the brand reputation and stock value.	

Acknowledgements This work was partially supported by the Colombian Navy, the Naval School "Admiral Padilla" (Colombia), the Fulbright Student Program of the U.S. Department of State, and the University of Rosario (Colombia).

Funding Open Access funding provided by Colombia Consortium

Declarations

Conflict of interest The authors declare that they have no Conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Departamento Nacional de Planeación - DNP, Documento CONPES 3995 - Política Nacional de Confianza y Seguridad Digital, (2020). [Online]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf
2. Argaw, S.T., Bempong, N.-E., Eshaya-Chauvin, B., Flahault, A.: The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med. Inf. Decis. Mak. **19**, 1–11 (2019)
3. Viganò, E., Loi, M., Yaghmaei, E.: Cybersecurity of critical infrastructure. In: Christen, M., Gordijn, B., Michele, L. (eds.) The International Library of Ethics, Law and Technology. The Ethics of Cybersecurity, pp. 157–177. Springer, Berlin (2020)
4. Bendovschi, A.: Cyber-attacks – trends, patterns and security countermeasures. In: Procedia Economics and Finance, ser. Proceedings of 7th International Conference on Financial Criminology ICFC (2015), vol. 28. Wadham College, Oxford University, United Kingdom: Elsevier, April 2015, pp. 24–31. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212567115010771
5. Liu, P.: Cyber situational awareness. In: Jajodia, S., Samarati, P., Yung, M. (eds.) Encyclopedia of Cryptography, Security and Privacy, pp. 1–3. Springer, Berlin (2019). https://doi.org/10.1007/978-3-642-27739-9_1768-1
6. Information Systems Audit and Control Association - ISACA, Risk IT Framework, 2nd Edition. ISACA, (2020). [Online]. Available: https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology
7. Martínez Martínez, I., Florián Quitián, A., Díaz-López, D., Nespoli, P., Gómez Mármol, F.: Malseirs: forecasting malware spread based on compartmental models in epidemiology. Complexity **2021**(1), 5415724 (2021)
8. Brauer, F.: Compartmental models in epidemiology. In: Brauer, F., van den Driessche, P., Wu, J. (eds.) Mathematical Epidemiology, pp. 19–79. Springer, Berlin (2008)https://doi.org/10.1007/978-3-540-78911-6_2
9. Nguyen, B.: Modelling cyber vulnerability using epidemic models. In Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications, ser. SIMULTECH 2017. Setubal, Portugal: SCITEPRESS - Science and Technology Publications, (2017), p. 232–239. [Online]. Available: https://doi.org/10.5220/0006401902320239
10. Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., Musharraf, M.: Developments and research directions in maritime cybersecurity: a systematic literature review and bibliometric analysis. Int J Crit Infrastruct. Prot. **39**, 100571 (2022)
11. Kuhn, K., Bicakci, S., Shaikh, S.A.: Covid-19 digitization in maritime: understanding cyber risks. WMU J. Marit. Aff. **20**(2), 193–214 (2021). (https://link.springer.com/article/10.1007/s13437-021-00235-1#citeas)
12. United Nations Conference on Trade and Development - UNCTAD, Review of Maritime Transport 2024. UNCTAD, (2024). [Online]. Available: https://unctad.org/system/files/official-document/rmt2024_en.pdf
13. Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A., Apostolou, P.: Digital transformation of the maritime industry: a cybersecurity systemic approach. Int. J. Crit. Infrastruct. Prot. **37**, 100526 (2022). (https://www.sciencedirect.com/science/article/pii/S1874548222000166)
14. Cabuya-Padilla, D.E., Castaneda-Marroquin, C.A.: Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - marcim: estado del arte y metodología. *DYNA*, **91**, no. 231, p. 169–179, ene. (2024). [Online]. Available: https://revistas.unal.edu.co/index.php/dyna/article/view/109774
15. Karim, M.S.: Maritime cybersecurity and the IMO legal instruments: sluggish response to an escalating threat? Mar. Policy **143**, 105138 (2022). (https://www.sciencedirect.com/science/article/pii/S0308597X22001853)
16. Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.-H.: Maritime cybersecurity: are onboard systems ready? Marit. Policy Manag. **51**(3), 484–502 (2024). (https://doi.org/10.1080/03088839.2022.2124464)
17. International Maritime Organization - IMO, *Guidelines on Maritime Cyber Risk Management*, (2022). [Online]. Available: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
18. Maritime Safety Committee.: Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. (2017). [Online]. Available: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428%2898%29.pdf
19. International Maritime Organization - IMO, Resolution MSC-FAL.1/Circ.3/Rev.2 - Guidelines on Maritime Cyber Risk Management, (2022). [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf
20. International Organization for Standardization—ISO.: ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements, ISO, (2022). [Online]. Available: https://www.iso.org/standard/27001
21. National Institute of Standards and Technology—NIST.: The NIST Cybersecurity Framework (CSF) 2.0, NIST, (2024). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
22. Baltic and International Maritime Council—BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners - INTERCARGO, InterManager, International Association of Independent Tanker

Owners - INTERTANKO, International Chamber of Shipping - ICS, International Union of Marine Insurance - IUMI, Oil Companies International Marine Forum - OCIMF, Superyacht Builders Association - SYBASS, and World Shipping Council - WSC, *The Guidelines on Cyber Security Onboard Ships*, (2020). [Online]. Available: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf
23. International Association of Classification Societies.: Recommendation on Cyber Resilience, IACS, 4 (2022). [Online]. Available: https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new-corr2-cln
24. International Association of Ports and Harbors—IAPH.: Cybersecurity guidelines for ports and port facilities. IAPH Head Office, Tech. Rep., 7 2021. [Online]. Available: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
25. Cabuya-Padilla, D.E., Castaneda-Marroquin, C.A.: Maritime cyberdefense actors taxonomy for command and control. In: Rocha, Á., Fajardo-Toro, C.H., Rodríguez, J.M.R. (eds.) Developments and Advances in Defense and Security, pp. 37–46. Springer, Singapore (2022)
26. Open Web Application Security Project Foundation—OWASP.: OWASP Risk Rating Methodology, OWASP, (2017). [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
27. Jabbour, K., Poisson, J.: Cyber risk assessment in distributed information systems. Cyber Def. Rev. **1**(1), 91–112 (2016). (http://www.jstor.org/stable/26267301)
28. Schlichting, A.D.: MITRE - Assessment of Operational Energy System Cybersecurity Vulnerabilities. In: The MITRE Corporation, Tech. Rep. January 2018, (2018). [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1108073.pdf
29. Information Systems Audit and Control Association—ISACA.: CISM Review Manual 16th Edition. ISACA, (2022)
30. Mehta, S., Yadav, V.: ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide, (2023)
31. Bjørnstad, O.N., Shea, K., Krzywinski, M., Altman, N.: Modeling infectious epidemics. Nat. Methods **17**(5), 455–457 (2020). (https://doi.org/10.1038/s41592-020-0822-z)
32. Li, M.Y., Muldowney, J.S.: Global stability for the SEIR model in epidemiology. Math. Biosci. **125**(2), 155–164 (1995). (https://www.sciencedirect.com/science/article/pii/0025556495927565)
33. Bjørnstad, O.N., Shea, K., Krzywinski, M., Altman, N.: The SEIRS model for infectious disease dynamics. Nat. Methods **17**, 557–558 (2020). (https://doi.org/10.1038/s41592-020-0856-2)
34. Kotenko, I.: Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in internet. In: 19th European Simulation Multiconference "Simulation in wider Europe, (2005). [Online]. Available: https://scs-europe.net/services/ecms2005/pdf/abs-03.pdf
35. Kotenko, I.: Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. In: 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, (2007), pp. 614–619. [Online]. Available: https://ieeexplore.ieee.org/document/4488494
36. Dobson, G.B., Carley, K.M.: Cyber-fit: an agent-based modelling approach to simulating cyber warfare. In: Lee, D., Lin, Y.-R., Osgood, N., Thomson, R. (eds.) Social, Cultural, and Behavioral Modeling, pp. 139–148. Springer, Cham (2017)
37. Hernández Guillén, J.D., Martín del Rey, A., Casado-Vara, R.: Security countermeasures of a sciras model for advanced malware propagation. IEEE Access **7**, 135 472-135 478 (2019)
38. Kavallieratos, G., Spathoulas, G., Katsikas, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors **21**(5), 1691 (2021)
39. Francia, G.A., III., Francia, X.P., Bridges, C.: Agent-based modeling of entity behavior in cybersecurity. In: Daimi, K., Peoples, C. (eds.) Advances in Cybersecurity Management, pp. 3–18. Springer, Cham (2021)https://doi.org/10.1007/978-3-030-71381-2_1
40. Estay, D.A.S.: A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities. J. Simul. **17**(1), 1–16 (2023). (https://doi.org/10.1080/17477778.2021.1890533)
41. Office of Strategic Services.: Simple sabotage field manual, Washington, D.C., (1944). [Online]. Available: https://www.cia.gov/static/5c875f3ec660e092cf893f60b4a288df/SimpleSabotage.pdf
42. Bochman, A.A., Freeman, S.: Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE). CRC Press, (2021). [Online]. Available: https://www.taylorfrancis.com/books/mono/10.4324/9780367491161/countering-cyber-sabotage-andrew-bochman-sarah-freeman
43. Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain. In: Abawajy, J.H., Mukherjea, S., Thampi, S.M., Ruiz-Martínez, A. (eds.) Security in Computing and Communications, pp. 438–452. Springer, Cham (2015)
44. Ganuza, N.: Cyber defense guide: Guidelines for the design, planning, implementation and development of a military cyber defense, Inter-American Defense Board, Washington D.C., (2020). [Online]. Available: https://jid.org/wp-content/uploads/2022/01/Cyber-defense_handbook_ing.pdf
45. Mandt, E.: Integrating cyber-intelligence analysis and active cyber-defence operations. J. Inf. Warf. **16**(1), 31–48 (2017)
46. Irfan, A.N., Chuprat, S., Mahrin, M.N., Ariffin, A.: Taxonomy of cyber threat intelligence framework. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), (2022), pp. 1295–1300. [Online]. Available: https://ieeexplore.ieee.org/document/9952616
47. Tirenin, W., Faatz, D.: A concept for strategic cyber defense. In: IEEE Military Communications. Conference Proceedings. MILCOM 1999, vol. 1, pp. 458–463 (1999). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/822725
48. Alsmadi, I.: The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics, pp. 69–84. Springer, Cham (2023)https://doi.org/10.1007/978-3-031-21651-0_5
49. Granova, A., Slaviero, M.: Cyber warfare. In: Computer and Information Security Handbook, third edition ed., J. R. Vacca, Ed. Boston: Morgan Kaufmann, pp. 1085–1104. (2017) [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128038437000831
50. Klimburge, A.: National cyber security framework manual, NATO CCD C ed., NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, (2012). [Online]. Available: https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/
51. Lété, B.: NATO and the EU: The essential partners, NATO Defense College, Tech. Rep., (2019). [Online]. Available: http://www.jstor.org/stable/resrep19964.9
52. Schmitt, M.N.: Tallinn manual 2.0 on the international law applicable to cyber operations, 2nd edn. Cambridge University Press, Cambridge (2017)https://doi.org/10.1017/9781316822524
53. Jabbour, K., Adams, S., Gorniak, M., Humiston, T., Hurley, P., Klumpe, H., Ratazzi, P., Repak, P., Sessler, B., Sidoran, J., et al.: The science and technology of cyber operations. High Front. **5**(3), 11–15 (2009)
54. Panfilov, A.V., ten Tusscher, K.H., de Boer, R.J.: Matrices, Linearization, and the Jacobian Matrix. Utrecht University, (2022). [Online]. Available: https://tbb.bio.uu.nl/rdb/books/math.pdf
55. Meador, C.-E.E.: Numerical calculation of lyapunov exponents for three-dimensional systems of ordinary differential equations. In: Ph.D. dissertation, Marshall University, (2011).

[Online]. Available: https://mds.marshall.edu/cgi/viewcontent.cgi?article=1105&context=etd
56. Wesley, D.T., Dau, L.A., Roth, A.: Cyberattack: The MAERSK Global Supply-Chain Meltdown. In: 2019, Northeastern University. Ivey Publishing. [Online]. Available: https://iveypubs.my.site.com/store/s/product/cyberattack-the-maersk-global-supplychain-meltdown/01t5c00000CwquXAAR
57. Abbatemarco, N., Salviotti, G., De Rossi, L., D'Ignazio, C.: Understanding leadership competencies in cyber crisis management: Insights from the maersk global supply chain meltdown. In: *Proceedings of the 57th Hawaii International Conference on System Sciences*, (2024). [Online]. Available: https://hdl.handle.net/10125/106892
58. Greenberg, A.: Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Knopf Doubleday Publishing Group, New York (2019)
59. Powell, A.: (2019) Implementing the lessons learned from a major cyber attack - black hat Europe (2019). Black Hat - Youtube. [Online]. Available: https://www.youtube.com/watch?v=wQ8HIjkEe9o
60. Aidan, J.S., Zeenia, and Garg, U.: Advanced Petya ransomware and mitigation strategies. In: 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), pp. 23–28. (2018). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8703323
61. Moller, A.P.: - Maersk. (2024) Maersk web page. Maersk. [Online]. Available: https://www.maersk.com/
62. Sawang, S.: Understanding crisis management in modern societies. In: Entrepreneurial Crisis Management: How Small and Micro-Firms Prepare for and Respond to Crises, pp. 1–16. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-25188-7_1
63. Rõigas, H.: Cyber war in perspective: Lessons from the conflict in Ukraine. In: Cusumano, E., Corbe, M. (eds.) A Civil-Military Response to Hybrid Threats, pp. 233–257. Springer, Cham (2018)https://doi.org/10.1007/978-3-319-60798-6_11