Modeling and Assessing the Impacts of Cyber Threats on Interdependent Critical Infrastructures

Valeria Bonagura[1], Chiara Foglietta[1], Stefano Panzieri[1](✉),
Massimiliano Rossi[2], Riccardo Santini[2], Monica Scannapieco[2],
and Luisa Franchina[3]

[1] University Roma Tre, Rome, Italy
stefano.panzieri@uniroma3.it
[2] National Cybersecurity Agency, Rome, Italy
[3] Hermes Bay, Rome, Italy

Abstract. Critical infrastructures are complex networks with physical, geographical, logical and cyber interdependencies whose disruption can cause serious impacts to citizenry and society. Meanwhile, the use of information and communications technology to manage physical processes in critical infrastructure assets has significantly increased their cyber attack surfaces. The increased threats have led to the creation of national and international cyber security agencies to promote awareness of cyber threats and coordinate responses to cyber attacks.

In 2019, Italy set up the National Security Perimeter for Cyber, a regulatory construct that stipulates measures for guaranteeing the safety and security of public and private entities that provide essential functions and services. The law associated with the regulatory construct requires the covered entities to accurately describe their networks, information and communications technology systems and related services. The 2021 Italian legislation that established the National Cybersecurity Agency requires all National Security Perimeter for Cyber entities to inform the national agency about their assets. The National Cybersecurity Agency also collects detailed infrastructure information as well as reports about cyber attacks from the entities.

This chapter describes an ongoing research effort that supports Italian legislative requirements. In particular, it demonstrates how the consequences of cyber threats can be assessed in complex scenarios using an agent-based simulator that evaluates the National Cybersecurity Agency model under ransomware and distributed-denial-of-service attacks on interconnected Italian infrastructures.

Keywords: Critical Infrastructure Modeling · Simulation · Cyber Attacks · Cyber Impacts · Italian National Security Perimeter for Cyber

1 Introduction

Modern control systems integrate physical processes with communications and computational resources that improve system efficiency and operational performance. In recent years, attention has focused on a particular class of control

Published by Springer Nature Switzerland AG 2024
J. Staggs and S. Shenoi (Eds.): ICCIP 2023, IFIP AICT 686, pp. 143–163, 2024.
https://doi.org/10.1007/978-3-031-49585-4_7

systems called cyber-physical systems. Several definitions have been proposed for cyber-physical systems and their functionalities [20]. However, their essential behavior is that they act independently, cooperatively or as "systems of systems."

From a practical control systems perspective, cyber-physical system behavior is characterized by nonlinear interactions between discrete phenomena (digital systems) and continuous phenomena (physical systems). Several techniques are required to capture and analyze behavior at the low level such as discrete control logic, communications and distributed computing effects as well as at the global level. While the integration improves system efficiency and operational performance, the threats posed by system intrusions by adversaries are elevated. Additionally, the increased amount of sensor data complicates the task of detecting malicious attacks.

Examples of cyber-physical systems include supervisory control and data acquisition (SCADA) systems, transportation networks, electric power generation and distribution networks, water and gas distribution networks, advanced communications systems and, more generally, critical infrastructures. The systems straddle the information technology (IT) and operational technology (OT) domains with cyber-physical security becoming a focus of attention due to the convergence of previously-disjointed security functions.

Operational technology security has historically lagged information technology security. This is largely because operational technology has prioritized safety and uptime without much regard for cyber security [19]. However, this situation must change on account of digital integration. Indeed, digital integration has increased the attack surfaces of critical infrastructure assets, causing them to be targeted by cyber attacks by malicious actors that leverage the ubiquitous connectivity provided by information technology to access and breach systems that were once thought to be impenetrable [9,18].

This situation has highlighted the fragility of cities, states and nations [1]. A well-cited example is the 2021 attack on Colonial Pipeline in the United States [7,15,16]. Unknown, well-resourced actors successfully targeted the gasoline transportation infrastructure. Although the company and the U.S. government cooperated to restore full capacity, the critical infrastructure was shut down for several days. The impacts were serious – 71% of gas stations in the Charlotte, North Carolina metropolitan area were short of or ran out of fuel.

The Colonial Pipeline attack is just one of many incidents reported around the world. Nation states have become cognizant of the serious cascading impacts of cyber attacks on critical infrastructure assets and, ultimately, on society. Analyzing the interdependencies between critical infrastructure assets at the regional, national and international levels are essential to understanding the consequences of adverse events. It is the responsibility of nation states to define appropriate cyber security strategies and institute regulatory constructs that will render critical infrastructure assets safe, secure and resilient to adverse events.

Recent reforms related to the Italian cyber ecosystem have led to the enactment of an Italian national law – National Security Perimeter for Cyber – that identifies key private and public entities in Italy, including critical infrastructure assets that perform essential functions or provide essential services, and endeavors to protect them from cyber attacks [25]. According to the law, every perimeter subject is required to inform the National Cybersecurity Agency of its information and communications technology (ICT) assets, networks, information systems and related services, and share data about cyber attacks and the effects observed on their infrastructure assets.

This chapter describes an ongoing research effort that supports the Italian legislative requirements. In particular, it demonstrates how the consequences of cyber threats can be assessed in complex scenarios using an agent-based simulator that evaluates the National Cybersecurity Agency model under chains of synthetic ransomware and distributed denial-of-service attacks on interconnected Italian infrastructures. The research leverages the mixed holistic reductionist approach, a hierarchical method that decomposes infrastructures into simple elements at multiple levels of abstraction [6]. The approach employs data drawn from the national security perimeter to generate an impact model of interconnected infrastructures for analyzing hypothetical scenarios. The agent-based CISIApro 2.0 simulator [4,13] implementing the mixed holistic reductionist approach is employed to convey the impacts of cyber attacks on interconnected infrastructures in terms of the confidentiality, integrity and availability (CIA) security triad.

2 Related Work

Critical infrastructure assets have achieved high degrees of interoperability due to the pervasive integration of information and communications technology to the point where interdependencies couple infrastructure assets regardless of their nature, type or geographic locations [22]. Due to the high degree of interoperability, it is vital to model critical infrastructure interdependencies to assess the consequences of adverse events such as natural disasters, failures and cyber attacks in terms of the CIA security triad. At this time, no single modeling tool fits every need. However, depending on the application and available information, some tools are more suitable than others.

EPANET2 is an open-source tool that is widely used to model water distribution systems [23]. The tool, which leverages network analysis and hydraulic simulation to model water system behavior over time, has been used to simulate the effects of cyber attacks on water distribution systems and identify potential vulnerabilities.

Ficco et al. [12] developed a hybrid, distributed simulation platform for conducting cyber security evaluations of large-scale critical infrastructure systems. The platform supports the integration of multiple simulated environments and the use of penetration testing and monitoring tools to evaluate complex, distributed experimental scenarios in the cloud.

The DOMINO simulation tool enables critical infrastructure asset managers to create and update questionnaires pertaining to the autonomy of their facilities in the absence of primary and alternative resources [14]. Asset managers are assisted in ensuring business continuity via an early warning system that provides alerts about potential problems. The DOMINO tool provides insights into potential cascading temporal and spatial impacts in training scenarios.

The Critical Infrastructure Program for Modeling and Analysis (CIPMA) is an Australian public-private sector approach that identifies and assesses critical infrastructure risks, recommends prioritization of investments and evaluates mitigation strategies and business continuity plans [5]. The communications, energy, water and transportation sectors have leveraged CIPMA to develop improved emergency management responses. CIPMA has also been used to study large-scale scenarios, including a cyclone in Queensland, gas supply disruption on the North West Shelf and submarine cable shelf/cable outages [2].

This research employs the CISIApro 2.0 agent-based simulator [4,13] to analyze the consequences of adverse events on interconnected infrastructures. In the CISIApro 2.0 simulator, each infrastructure is decomposed into agents that describe complex behaviors. Details about the CISIApro 2.0 simulator are provided in Sect. 5.2.

3 National Security Perimeter for Cyber

A nation state is responsible for defining strategies focused on planning, coordinating and implementing measures that ensure the country's cyberspace is secure, safe and resilient while ensuring its citizenry can leverage the competitive advantages of cyberspace with complete protection of their fundamental rights and freedoms.

Since 2013, the Italian Government has invested considerable effort to keep pace with technological advances in the cyber domain. Over time, it has instituted a number of measures designed to acquire, develop and strengthen national cyber capabilities, and to guarantee institutional uniqueness of direction and action with respect to cyber security as an area of intervention that is national in scale and engages all stakeholders.

At the European Union (EU) level, the EU Network and Information Security (NIS) Directive 2016/1148 [11] specifies measures intended to achieve a "high level of security of network and information systems in the national sphere, contributing to increase the common level of security in the European Union." The directive was adopted into Italian law by Legislative Decree of May 18, 2018 (L.D. no. 65/2018) [24], which dictates the legislative framework of measures for securing networks and information systems and identifies the entities responsible for implementing the obligations under the EU NIS Directive.

This section highlights the Italian National Security Perimeter for Cyber Law [25] as a regulatory construct that covers more entities than the EU NIS directive and incorporates more compulsory rules. Following this, the section introduces recent Italian cyber ecosystem reforms.

On September 21, 2019, Law Decree no. 105/2019 – Urgent Measures Concerning the National Security Perimeter for Cyber (and Special Powers of the Government in the Strategic Sectors) [25] – was enacted by the Italian Government. The decree established the "National Security Perimeter for Cyber" that introduces measures to guarantee safety standards for networks and information systems as well as information technology services for public administrations, private and public entities and critical infrastructure assets that perform essential state functions or provide essential services in the civil, social and economic domains and whose malfunction may pose risks to national security.

The legislation has established provisions that are implemented via four Prime Ministerial Decrees and a Presidential Decree in order to:

- Identify the public and private entities falling within the National Security Perimeter for Cyber and the criteria for creating the lists of networks, information systems and relevant services (DPCM no. 131/2020) [26].
- Define the procedures for the notification of cyber incidents to the Computer Security Incident Response Team of Italy that impact networks, information systems and information services (DPCM no. 81/2021) [28].
- Define the evaluation procedures for information and communications technology assets used in the National Security Perimeter for Cyber and notify the National Assessment and Certification Center in charge of conducting security assessments with the goal of verifying the absence of known vulnerabilities in information and communications technology assets, systems and services (DPR no. 54/2021) [27].
- Identify the categories of information and communications technology assets, systems and services used by the entities included in the National Security Perimeter for Cyber and the procurement of communications technology assets evaluated by the National Assessment and Certification Center (DPCM no. 198/2021) [30].
- Define the accreditation procedures for Accredited Evaluation Laboratories and coordination procedures for the National Assessment and Certification Center, Accredited Evaluation Laboratories and Evaluation Centers belonging to the Italian Ministry of Defense and Italian Ministry of the Interior (DPCM no. 92/2022) [31].

These goals are being pursued through recent reforms of the national cyber ecosystem enacted by the Legal Decree of June 14, 2021 (L.D. no. 82/2021) [29]. The decree established the National Cybersecurity Agency of Italy with the mission of rationalizing and consolidating the fragmented expertise existing at the national level in compliance with the competencies attributed to other administrations by legislation in force, and further enhancing the cyber security and resilience for the purposes of protecting national security in cyberspace. As the national authority, the National Cybersecurity Agency of Italy develops the National Cybersecurity Strategy [21].

Furthermore, pursuant to L.D. no. 82/2021 [29], the National Cybersecurity Agency of Italy is designated as the exclusive competent national authority and single point of contact for the purposes referred to in the legislation on the security of networks and information systems (NIS) [11], National Cybersecurity Certification Authority, National Coordination Center with reference to the European Cybersecurity Competence Centre and Network [8] and central element of the National Security Perimeter for Cyber. It should be noted that these competencies were previously attributed to a plurality of institutional actors and that the Computer Security Incident Response Team of Italy and National Assessment and Certification Center are established within the National Cybersecurity Agency.

4 Ontology-Based Approach

Decree of the President and the Council of Council of Ministers of July 30, 2020 (DPCM no. 131/2020) [26] assigns to every public and private entity in the National Security Perimeter for Cyber the mandatory duty to inform the National Cybersecurity Agency of its information and communications technology networks, information systems and related services by compiling a comprehensive list. To support these entities, the National Cybersecurity Agency has designed a formal model for accurately describing all the relevant assets (e.g., information systems, routers and services) and their relationships (e.g., structures and dependencies). The model captures the characteristics of the two key domains in which the entities perform essential state functions and/or provide essential information and communications technology and operational technology services.

The National Cybersecurity Agency model can be viewed as an ontology because it formalizes domain knowledge in a structured manner using two types of components. The first component type is entities, which are defined as classes of objects of interest with homogeneous characteristics along with their related properties. The second component type is the relationships between entities.

A domain is described by accurately defining the entity instances along with their characteristic properties and relationships. Additionally, the model enables the expression of the applicable constraints.

The National Cybersecurity Agency model, which is called the perimeter ontology, has four logical sections:

- Entity description, information and communications technology functions and/or services, and the relationships between them.
- Information and communications technology networks, systems and services, hardware and software components and nodes. Nodes are components collected in physical or logical spaces such as data centers and electrical substations.
- Outgoing dependencies such as external services on which entities depend.
- Geographical locations of all the components listed above.

Details about the perimeter ontology are not provided in this chapter for national security reasons. The complete lists of networks, information systems and services pertaining to the entities are also protected by confidentiality clauses.

However, the authors of this chapter believe that it is important to present the approach for collecting perimeter data in a structured manner using an ontology. The approach has three principal advantages. One is ambiguity reduction at the data sources because the semantics of the collected data is formally specified at the data collection stage. The second is the reduction of the complexity of the steps following data collection, especially related to the storage and analysis of the collected data. The third is the quality (completeness) of the collected data due to the use of well-defined and somewhat rigid collection tools.

5 Modeling Approach

This section describes the mixed holistic reductionist approach for modeling interdependent critical infrastructures. Also, it describes the CISIApro 2.0 simulator that is designed to assess the impacts of adverse events in complex modeled critical infrastructure scenarios.

5.1 Mixed Holistic Reductionist Approach

The mixed holistic reductionist approach leverages the benefits of holistic and reductionist thinking [6]. The approach provides a roadmap for meticulously modeling critical infrastructures and their interdependencies.

The mixed holistic reductionist approach describes interconnected infrastructures as a set of networks. Each infrastructure is described at different abstraction levels to capture phenomena that emerge at different granularities. The idea is to integrate the advantages of the holistic and reductionist approaches.

Infrastructures are viewed as distinct entities with clearly-defined borders and functional attributes in holistic modeling to provide a comprehensive and global picture. When considering an infrastructure as a whole, it is possible to identify and describe the infrastructures as well as their regional reaches. At this level, the amount of data required for modeling operations is small and may be available in open databases.

On the other hand, the reductionist paradigm emphasizes the need to carefully study the roles and behaviors of individual components to fully understand the entire system. Specifically, the reductionist approach breaks down each component into its inputs and outputs. Relations between machinery and individual parts are easily specified at this level of abstraction.

Service efficiency (referred to as “service”) functions as the link between the holistic and reductionist levels. This layer describes the functional connections between infrastructures and components at varying granularities. Consumers and other connected infrastructures reside in the middle layer between the holistic and reductionist levels.

Different systems require different levels of analysis, and their limitations are lost in complex case studies. The mixed holistic reductionist approach allows for top-down or bottom-up analyses of network interactions at various levels. It also enables critical infrastructures to be modeled at different degrees of abstraction based on the available data.

Figure 1 shows a mixed holistic reductionist model representation starting from the perimeter ontology. The central nodes are in the holistic layer, the dark

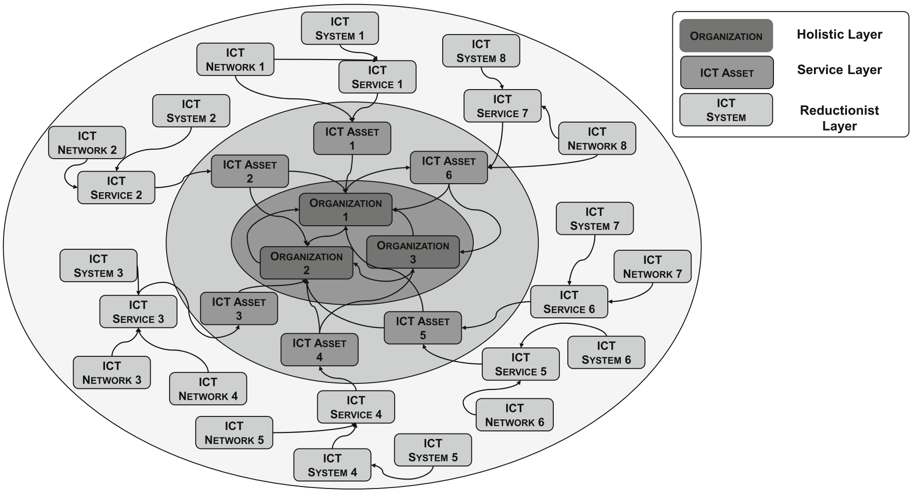

Fig. 1. Mixed holistic reductionist model representation.

grey nodes are in an intermediate layer and the external nodes are in the reductionist layer. The transition from the ontology to the mixed holistic reductionist model is not obvious, and human intervention is required to resolve conflicts between the two views. The model shown in Fig. 1 is the original proposal for modeling interdependencies and lacks direct correspondence with the ontology in terms of entities and relationships.

The holistic layer contains all the agents representing all the entities that are part of the perimeter or are directly linked to an entity in the perimeter. Due to the difficulty of determining the particular devices on which connections occur, the corresponding agents are connected among themselves primarily to exchange cyber risk. Cyber risks are related to cyber attack impacts, which are primarily confidentiality and integrity (a data breach at an entity has no direct impact on information availability, but it can impact the entity's trust and reputation at the holistic level). When data is not available, the model may contain blocks related to the entity without additional details.

An entity provides essential services to its customers and other entities. Each service is produced by an information and communications technology asset. Therefore, each service layer contains agents called information and communications technology assets that represent parts of the information and communications technology network that are necessary to deliver essential services. Entity blocks are linked to information and communications technology assets in two ways. The first corresponds to the information and communications technology assets of an infrastructure that provide resources, faults and cyber attacks to the entity blocks associated with the same infrastructure. The second corresponds to the information and communications technology assets that produce specific resources (services) used by other infrastructures.

As shown in Fig. 1, an information and communications technology asset comprises systems, networks and services. The three categories represent devices (hardware and software) that are fundamental to delivering services. These elements are part of the reductionist layer of the model. Hence, the blocks represent the information and communications technology portions of the operational technology environment. Note that all the blocks are not depicted in the figure. The reductionist layer contains some blocks that are cyber-physical components such as data centers, buildings and electrical substations. A cyber-physical system incorporates several components needed to produce a service, but also contains some information and communications technology components.

The case study described in this chapter also considers the possibility of infrastructures that are interconnected at all the layers in the model. For instance, an airline company, which is considered to be a reductionist component, depends on electricity supplied by a utility whose information and communications technology assets need bank services to collect payments from customers. However, impacts such as confidentiality, integrity and availability are exchanged at the entity level, namely, at the holistic layer.

5.2 CISIApro 2.0 Simulator

The Critical Infrastructure Simulator with Interdependent Agents 2.0 (CISIApro 2.0) [4,13] is employed to evaluate the consequences of adverse events on interconnected critical infrastructures. The simulator engages agent-based modeling using three main components, agents, simple interaction rules and the environment in which the agents are placed. Multiple agents acting simultaneously according to the interaction rules model complex systems. In agent-based modeling, central control does not drive agent behavior. Instead, following the local rules leads to an outcome or aggregate behavior that adapts to the environment or reacts to adverse situations. Thus, an agent-based model is a simply a set of agents that follow simple rules to collectively generate an emergent property or behavior. The main drawback of agent-based modeling is that it requires high levels of detail to provide adequate predictions. As a result, the accuracy of agent-based modeling depends on the specificity of the underlying assumptions.

Figure 2 shows the CISIApro 2.0 agent representation. Each infrastructure is decomposed into agents with the same overall input and output structures. Each agent receives resources, faults and cyber attacks from upstream agents and sends resources, faults and cyber attacks to downstream agents. Resources are supplies of materials, quantities and other assets that are required by entities to function effectively. Faults include malfunctions and natural events that must be exploited to assess different outcomes, depending on the details of the initial adverse events. Cyber attacks are malicious activities that attempt to collect, disrupt, deny, degrade or destroy information and communications technology resources. In a CISIApro 2.0 simulation, resources, faults and cyber attacks are exchanged among agents.

Agent state is identified by its operational level. The operational level indicates an agent's ability to function properly and execute its tasks. Every agent

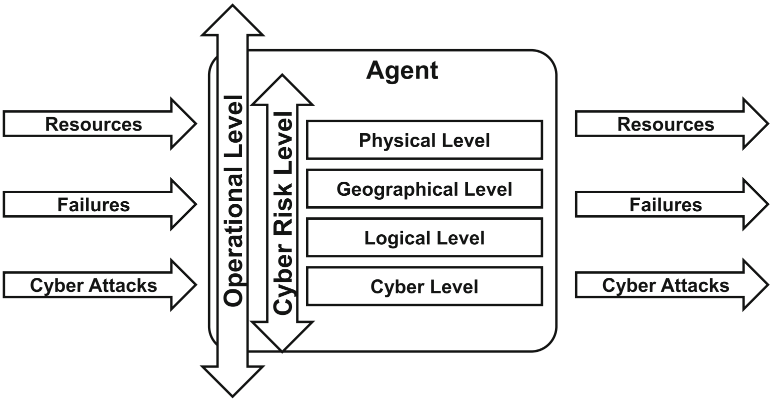

Fig. 2. CISIApro 2.0 agent representation.

has an internal state variable that represents its internal behavior based on the evaluation of resources, faults and cyber attacks. Based on its operational level, each agent sends resources, faults and cyber attacks to downstream agents.

To better handle cyber attacks and evaluate their consequences, each agent has an additional state variable called the cyber risk level that identifies how the agent is affected by internal and incoming cyber attacks. Cyber risk is based on the CIA triad. The CIA triad may be difficult to apply in industrial automation and control environments, but the three security goals are useful to deal with information in classical information technology environments and to spread information about cyber attacks in industrial automation and control environments. In fact, the CIA triad is invaluable when it comes to determining the impacts of cyber attacks on the telecommunications network portions of industrial automation and control systems.

It is instructive to clarify the meanings of the CIA terms and their relationships in industrial automation and control environments. Real-time processes at Purdue levels 0 to 2 [3,32] are often exempt from the confidentiality requirement because operational and real-time parameters are not viewed as secrets. Secret manufacturing formulas are to be protected and this must be done in the information technology and industrial automation and control zones [17]. Since real-time operating data has not been tampered with, it can be trusted. However, the industrial automation and control zone is viewed as being insecure by design. Therefore, by employing trustworthy design, perimeter security and supplemental cyber security, the integrity of the industrial automation and control zone can be guaranteed.

Dependability, productivity and business continuity standards for the industrial automation and control zone also address availability. Similar to integrity, availability must be guaranteed through trustworthy architectures, dependable goods and trustworthy software.

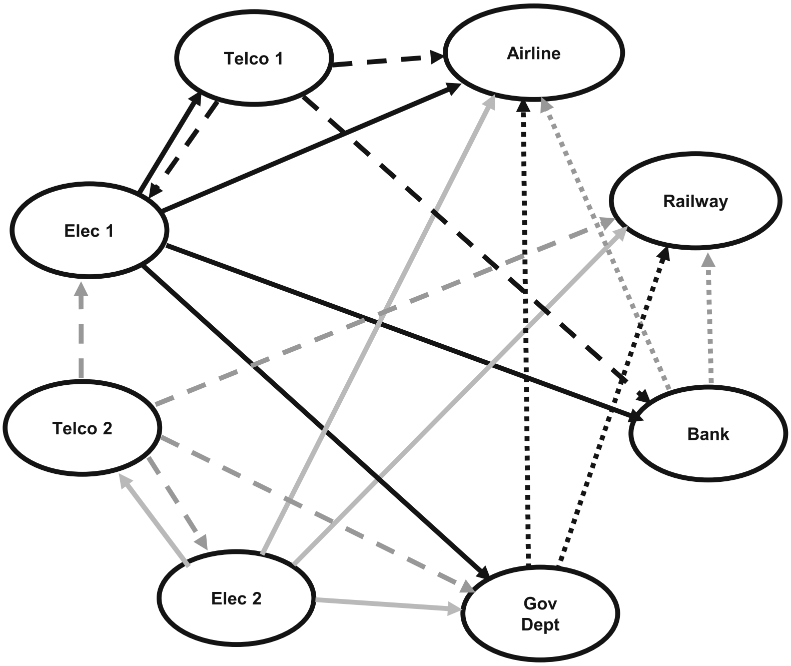

Fig. 3. Interdependencies between the interconnected infrastructures.

In a CISIApro 2.0 simulation, the availability of information transmitted by a telecommunications network is captured by its operational level. In contrast, confidentiality and integrity are expressed as cyber risk levels. As shown in Fig. 2, the operational and cyber risk level metrics may be interconnected and partially overlap.

6 Case Study

A case study involving eight interconnected infrastructures is used to demonstrate the efficacy of the mixed holistic reductionist approach and CISIApro 2.0 simulation. The interconnected infrastructures include two telecommunications companies, two electrical power distribution companies, a railway company, an airline company, a bank and a government department.

Figure 3 shows the interdependencies between the eight interconnected infrastructures. The two telecommunications companies provide services such as Internet access and mobile and backbone telecommunications. The two electrical power distribution companies provide electricity for equipment as well as to buildings, railway stations and airports. The bank processes customer payments to the railway and airline companies. The government department issues licenses for rail transport of people and goods and regulates airline company operations.

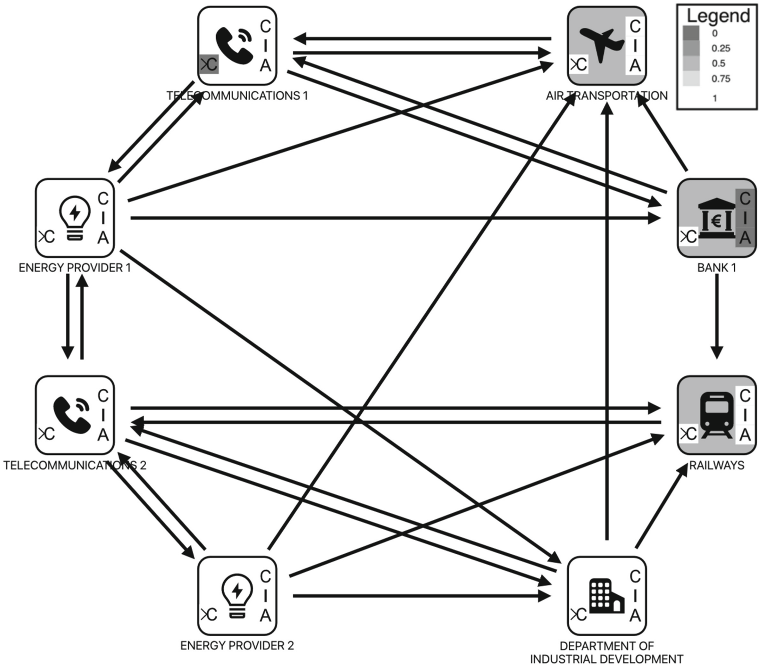

Fig. 4. Bank infrastructure view after the ransomware attack.

6.1 Ransomware Attack

The first scenario involves a ransomware attack on customer payment services provided by the bank. A ransomware attack enables an adversary to seize control of the targeted assets and demand a ransom in exchange for availability of the assets [9,10]. In 2022, ransomware was one of the top cyber threats, affecting all sectors indiscriminately and with numerous high-profile cases [10].

Figure 4 shows the bank infrastructure view after the ransomware attack. The ransomware disrupts the bank services that process customer payments to the railway and airline companies. All the entities have the operational levels expressed by the gray scale in the icon backgrounds, the CIA triads on the right-hand sides of the icons and the cyber risk due to the interconnected infrastructures indicated by $> C$ in the bottom-left corners of the icons.

As expected, the ransomware attack causes drastic reductions in the three components of the CIA triad at the bank. However, no impacts are observed on the primary transportation functions of the railway and airline companies; as a result, the operative levels of the two companies are 0.5. Additionally, the possibility exists that the attack impacts the telecommunications company providing services to the bank when the adversary conducts lateral movements and exploits vulnerabilities to enter and control remote systems in the interconnected telecommunications network.

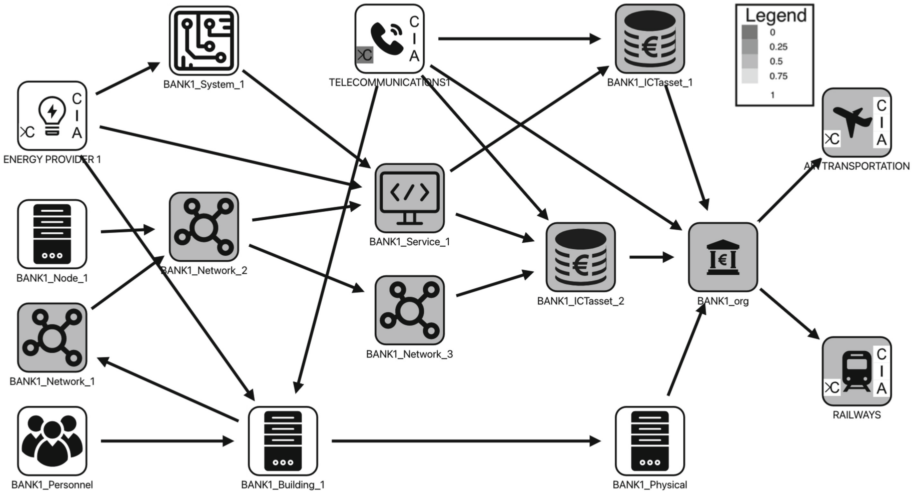

Fig. 5. High-level bank representation.

Figure 5 shows the high-level representation of the bank. Since the ransomware attack targets an information and communications technology service common to the two information and communications technology assets at the bank, the operational level of the bank drops to zero.

The railway company (Fig. 6) and airline company (Fig. 7) are also affected partially by the ransomware attack. The impacted services at the two companies primarily relate to ticket sales. Specifically, the two companies rely on telecommunications and bank services for ticket sales and the observed impact is mainly on the transactions. The combination of the services supplied by the two information and communications technology assets is evaluated using the average operation. The operational levels of the railway and airline companies are both equal to 0.5, where one corresponds to fully operational.

As mentioned above, the information and communications technology systems and networks of the bank and telecommunications company are linked. Thus, due to lateral movements and the exploitation of vulnerabilities by the adversary, the telecommunications company may be affected in a different manner by the ransomware attack.

Figure 8 shows the impact on the telecommunications company due to lateral movements from the bank network and vulnerability exploitation. The telecommunications network does not have a direct impact on the functional level; instead, the impact is on company trust and reputation. The operational level of the telecommunications company is one because there is no impact on telecommunications services.

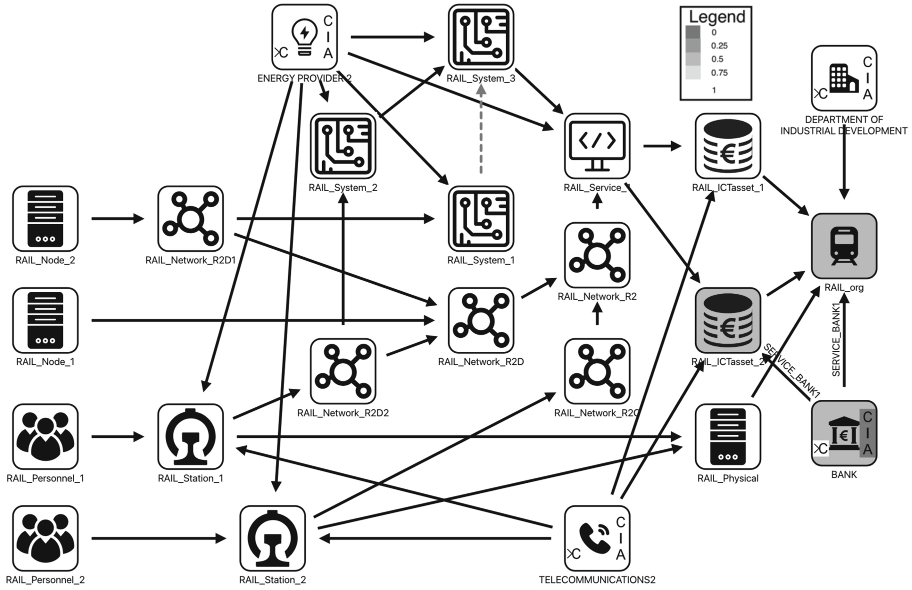

Fig. 6. Railway company representation.

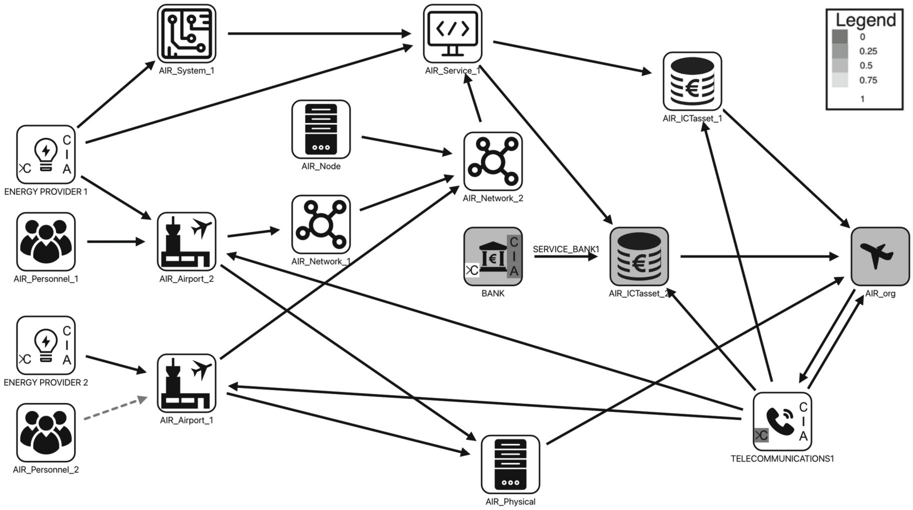

Fig. 7. Airline company representation.

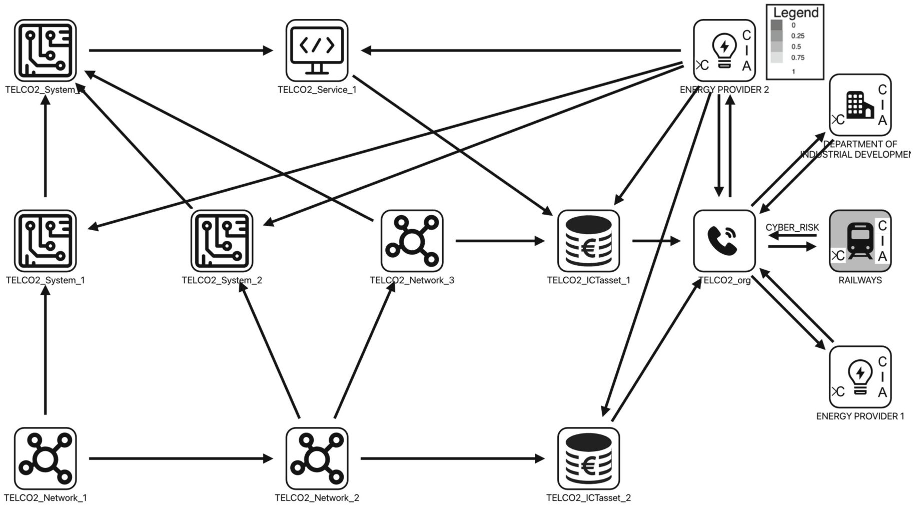

Fig. 8. Telecommunications company representation.

6.2 Distributed Denial-of-Service Attack

A denial-of-service attack directly impacts the availability of computer and network resources, causing temporary problems for customers who rely on services. A typical denial-of-service (DoS) attack floods a target with traffic or sends information that triggers a crash. A distributed denial-of-service (DDoS) attack occurs when multiple systems orchestrate a synchronized denial-of-service attack on a single target. The main difference is that, instead of being attacked from one location, the target is attacked simultaneously from multiple locations. Distributed denial-of-service was ranked the most serious cyber threat in 2022 whereas ransomware was ranked the most serious cyber threat in 2021 [9].

Figure 9 shows a synoptic view of the infrastructures after a distributed denial-of-service attack on an information and communications technology service agent at the second telecommunications company. As expected, the telecommunications service disruption has a profound impact on all the other interconnected infrastructures.

Figure 10 shows the impact of the distributed denial-of-service attack on the second telecommunications company. All the services provided by the company are affected. The situation is more serious than the one shown in Fig. 8. This is because the second telecommunications company provides services to the two electric power distribution companies, railway company and government department.

Figure 11 shows the impact of the telecommunications distributed denial-of-service attack on the railway company. Railway operations are highly impacted by the telecommunications service disruption because the company has only one telecommunications provider whose services are used to coordinate information

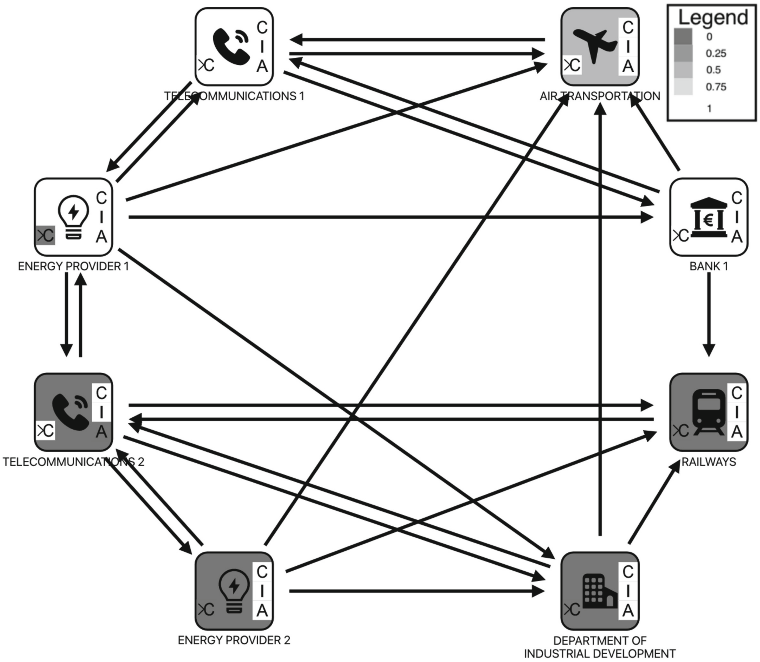

Fig. 9. Overall impact of DDoS attack on telecommunications company.

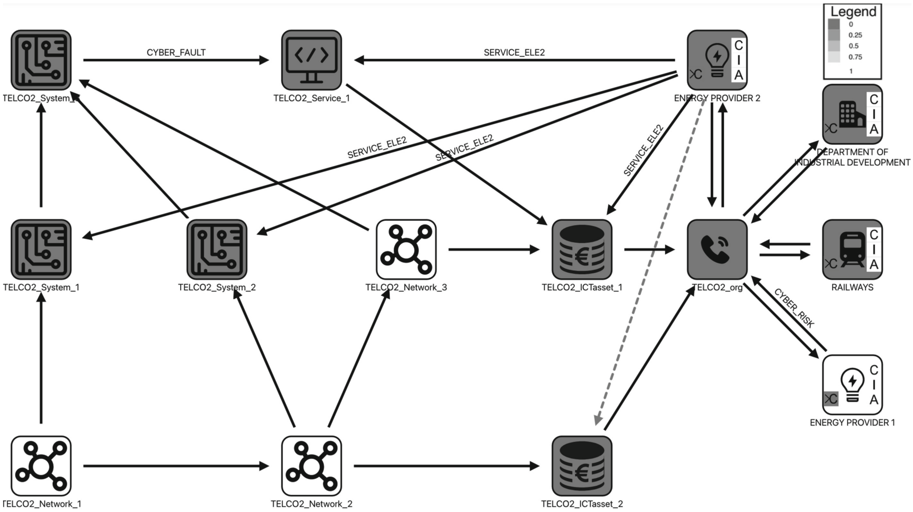

Fig. 10. Impact of DoS attack on telecommunications company.

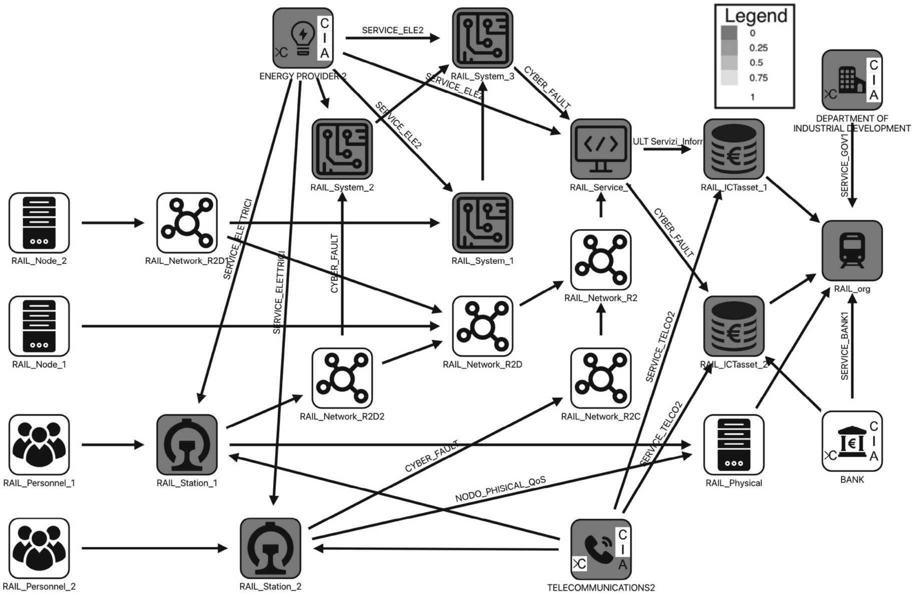

Fig. 11. Impact of telecommunications DDoS attack on railway company.

and communications systems and services at two railway stations. The railway company is also potentially impacted by the disruption of electricity from its electric power distribution company that receives services from the targeted telecommunications company.

The government department relies on telecommunications services to perform its functions. Figure 12 shows that the telecommunications distributed denial-of-service attack impacts the government department building as well as its two information and communications technology assets.

Figure 13 shows the impact of the telecommunications distributed denial-of-service attack on electric power distribution. The two electric power distribution companies have different supply chains. The company shown in Fig. 13 has a single telecommunications service provider whereas the other company has two telecommunications service providers. As a result, the impacts are completely different. The impact on the first company is significant whereas the second company is not affected.

The impact of the telecommunications distributed denial-of-service attack on the electric power distribution company in Fig. 13 leads to negative impacts on other infrastructures. The railway system needs electricity for its information and communications technology systems (Fig. 11) and the airline company needs electricity for one of the two airports (Fig. 14).

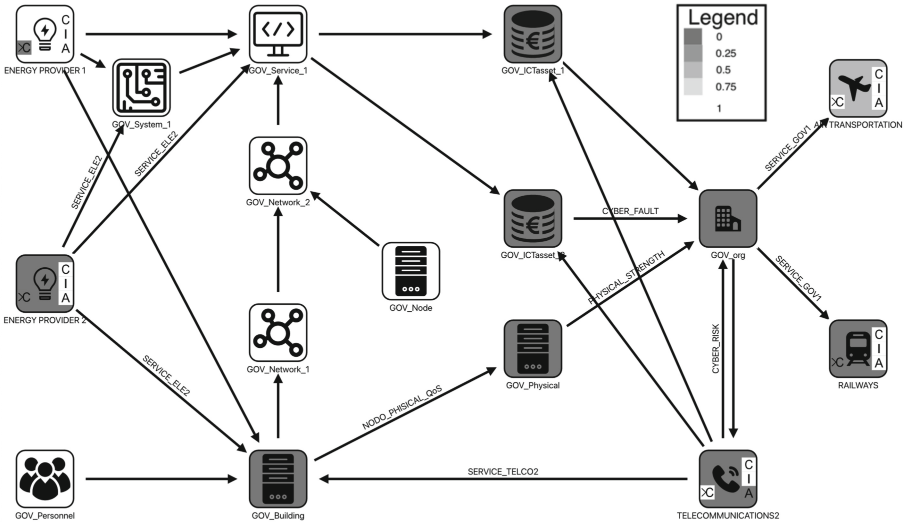

Fig. 12. Impact of telecommunications DDoS attack on government department.

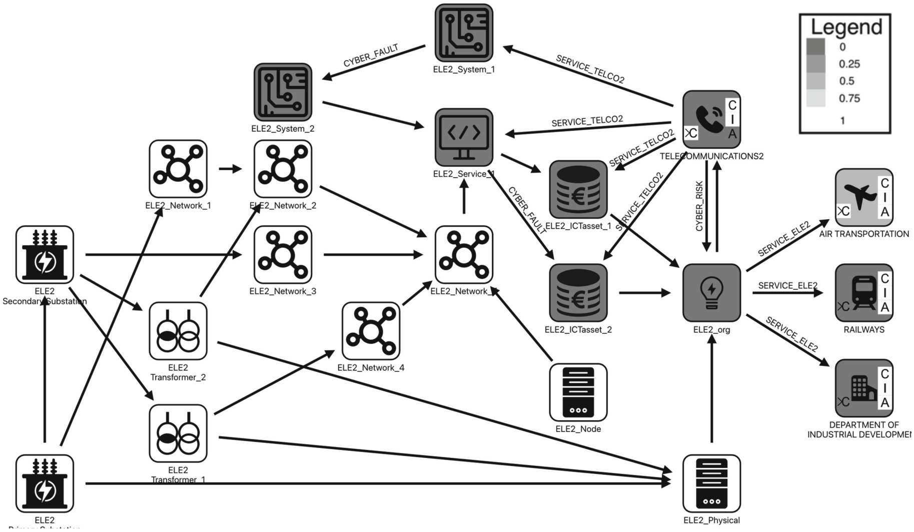

Fig. 13. Impact of telecommunications DDoS attack on electric power distribution.

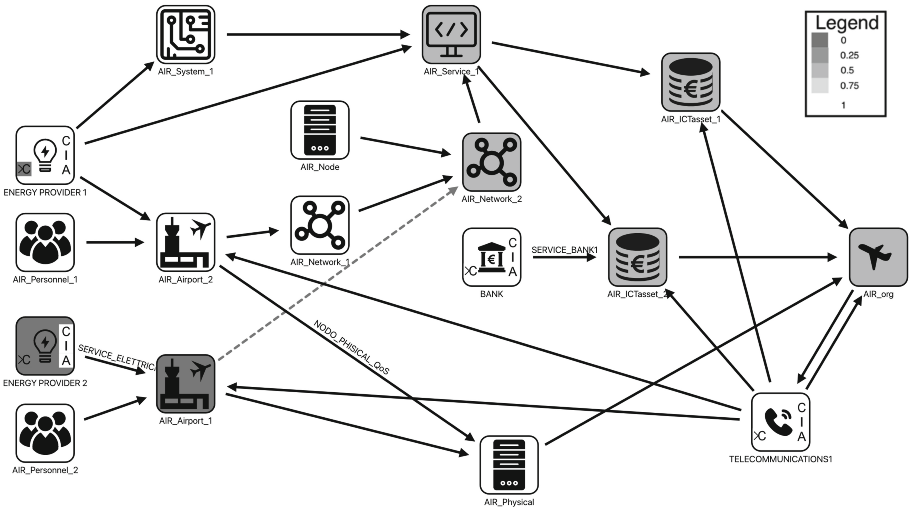

Fig. 14. Impact of telecommunications DDoS attack on airline company.

7 Conclusions

Nation states have become cognizant of the serious cascading impacts of cyber attacks on critical infrastructure assets and, by extension, on society. The increased threats have led to the creation of national and international cyber security agencies to promote awareness of cyber threats and coordinate responses to cyber attacks. By law, all the public and private entities in the Italian National Security Perimeter for Cyber must inform the National Cybersecurity Agency about all their information and communications technology assets, networks, information systems and services. This information is submitted using an ontology provided by the National Cybersecurity Agency. However, modeling interdependent infrastructures and assessing the impacts of cyber attacks are complex problems.

This chapter has demonstrated how the mixed holistic reductionist approach can be employed to decompose each infrastructure into different abstraction layers, model their interdependencies and evaluate the effects of adverse events. By employing the mixed holistic reductionist approach with the ontology proposed by the Italian National Security Agency, the CISIApro 2.0 agent-based simulator can be used to model complex cyber scenarios involving the Italian National Security Perimeter for Cyber. The case study shows that the proposed approach can effectively assess the consequences of ransomware and distributed denial-of-service attacks on the connected infrastructures in terms of confidentiality, integrity and availability.

Future research will model additional interconnected infrastructures. The model will also be enhanced by considering propagation delays involving the data exchanged between infrastructures and the interactions between physical processes and information and communications technology services.

References

1. Alladi, T., Chamola, V., Zeadally, S.: Industrial control systems: cyberattack trends and countermeasures. Comput. Commun. **155**, 1–8 (2020)
2. Amélie, G., Aurélia, B., Emmanuel, L., Mohamed, E., Gilles, D.: The challenge of critical infrastructure dependency modelling and simulation for emergency management and decision making by the civil security authorities. In: Rome, E., Theocharidou, M., Wolthusen, S. (eds.) CRITIS 2015. LNCS, vol. 9578, pp. 255–258. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-33331-1_23
3. Assante, M., Lee, R.: The Industrial Control System Cyber Kill Chain, White Paper, SANS Institute, Bethesda, Maryland (2015)
4. Bernardini, E., Foglietta, C., Panzieri, S.: Modeling telecommunications infrastructures using the CISIApro 2.0 simulator. In: ICCIP 2020. IAICT, vol. 596, pp. 325–348. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62840-6_16
5. Cyber and Infrastructure Security Centre, CIPMA: Critical Infrastructure, Program for Modeling and Analysis, Australian Department of Home Affairs, Canberra, Australia (2015)
6. Digioia, G., Foglietta, C., Panzieri, S., Falleni, A.: Mixed holistic reductionistic approach for impact assessment of cyber attacks. In: Proceedings of the European Intelligence and Security Informatics Conference, pp. 123–130 (2012)
7. Dudley, R., Golden, D.: The Colonial Pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms, ProPublica (24 May 2021)
8. European Cybersecurity Competence Centre and Network, Bucharest, Romania (2023). (cybersecurity-centre.europa.eu/index_en)
9. European Network and Information Security Agency, ENISA Threat Landscape 2022, Heraklion, Greece (2022) (www.enisa.europa.eu/publications/enisa-threat-landscape-2022)
10. European Network and Information Security Agency, ENISA Threat Landscape for Ransomware Attacks, Heraklion, Greece (2022). (www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks)
11. European Parliament and the Council of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, Document 32016L1148, Brussels, Belgium (2016)
12. Ficco, M., Choras, M., Kozik, R.: Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. J. Comput. Sci. **22**, 179–186 (2017)
13. Foglietta, C., Panzieri, S.: Resilience in critical infrastructures: the role of modeling and simulation. In: Rosato, V., Di Pietro, A. (eds.) Issues on Risk Analysis for Critical Infrastructure Protection, IntechOpen, London, United Kingdom, pp. 3–18 (2020)
14. Franchina, L., Socal, A.: Innovative predictive model for smart city security risk assessment. In: Proceedings of the Forty-Third International Convention on Information, Communications and Electronic Technology, pp. 1831–1836 (2020)
15. Goodell, J., Corbet, S.: Commodity market exposure to energy-firm distress: evidence from the colonial pipeline ransomware attack. Finance Res. Lett. **51**, 103329 (2023)

16. Hobbs, A.: The Colonial Pipeline hack: Exposing vulnerabilities in U.S. cybersecurity, SAGE Business Cases (6 July 2021)
17. International Electrotechnical Commission, IEC 62443 Series - Industrial Communication Networks - Network and System Security, Geneva, Switzerland, 2009–2023
18. Katagiri, N.: Hackers of critical infrastructure: expectations and limits of the principle of target distinction. Inter. Rev. Law Comput. Technol. article no. 2164462 (2023)
19. Knowles, W., Prince, D., Hutchison, D., Pagna Disso, J., Jones, K.: A survey of cyber security management in industrial control systems. Inter. J. Critical Infrastructure Protect. **9**, 52–80 (2015)
20. Miclea, L., Sanislav, T.: About dependability in cyber-physical systems. In: Proceedings of the Ninth East-West Design and Test Symposium, pp. 17–21 (2011)
21. National Cybersecurity Agency, National Cybersecurity Strategy 2022 – 2026, Rome, Italy. (2022) (www.acn.gov.it/ACN_EN_Strategia.pdf)
22. Oliva, G., Panzieri, S., Setola, R.: Modeling and simulation of critical infrastructures. WIT Trans. State-of-the-Art Sci. Eng. **54**, 39–56 (2012)
23. Pathirana, A.: EPANET2 desktop application for pressure-driven demand modeling. In: Proceedings of the Twelfth Annual Conference on Water Distribution System Analysis, pp. 65–74 (2010)
24. Republic of Italy, Legislative Decree of May 18, 2018, no. 65 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, L.D. no. 65/2018, Rome, Italy (2018). (www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg)
25. Republic of Italy, Law Decree of September 21, 2019, no. 105 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, L.D. no. 105/2019, Rome, Italy (2019). (www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg)
26. Republic of Italy, Decree of the President and the Council of Ministers of July 30, 2020, no. 131 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, DPCM no. 131/2020, Rome, Italy (2020). (www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg)
27. Republic of Italy, Decree of the President of the Republic of February 5, 2021, no. 54 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, DPR no. 54/2021, Rome, Italy (2021). (www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg)
28. Republic of Italy, Decree of the President and the Council of Ministers of April 14, 2021, no. 81 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, DPCM no. 81/2021, Rome, Italy (2021). (www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg)
29. Republic of Italy, Legal Decree of June 14, 2021, no. 82 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, L.D. no. 82/2021, Rome, Italy (2021). (www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg)
30. Republic of Italy, Decree of the President and the Council of Ministers of June 15, 2021, no. 198 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, DPCM no. 198/2021, Rome, Italy (2021). (www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg)
31. Republic of Italy, Decree of the President and the Council of Ministers of May 18, 2022, no. 92 (in Italian), *Gazzeta Ufficiale della Repubblica Italiana*, DPCM no. 92/2022, Rome, Italy (2022). (www.gazzettaufficiale.it/eli/id/2022/07/15/22G00099/sg)
32. Williams, T.: The Purdue enterprise reference architecture. Comput. Ind. **24**(2–3), 141–158 (1994)