CHAPTER 19

Security and Resilience in Critical Infrastructures

Maria Belesioti, Rodoula Makri, Panos Karaivazoglou, Evangelos Sfakianakis, Ioannis Chochliouros, and Alexandros Kyritsis

19.1 Threats and Resilience in Critical Infrastructures

19.1.1 Introduction

Critical infrastructures (CIs) are valuable assets for a well-organized state and for a structured society. Within the global digital reality, CIs have become pure "enablers" for growth and development at a multiplicity of

M. Belesioti (✉) · E. Sfakianakis · I. Chochliouros
Hellenic Telecommunications Organization (OTE) S.A.,
Fixed Network R&D Programs Section, Athens, Greece
e-mail: mbelesioti@oteresearch.gr; esfak@oteresearch.gr;
ichochliouros@oteresearch.gr

R. Makri · P. Karaivazoglou · A. Kyritsis
Microwaves and Fiber Optics Lab, Institute of Communication and Computer Systems (ICCS) of the National Technical University of Athens, Athens, Greece
e-mail: rodia@esd.ece.ntua.gr; pkaraiv@esd.ece.ntua.gr

B. Akhgar et al. (eds.), *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement,
https://doi.org/10.1007/978-3-030-69460-9_19

levels and everyday life. However, CIs are “prime” targets for man-made threats, operation disruption, and organized terrorist attacks but can also be affected by extreme weather events and natural disasters.

A vast literature exists concerning the threats and vulnerabilities in CIs yielding a large discussion concerning their classification. Although various schemes are defined, it is seen that all aim to initiate suitable implementation of corresponding measures with an ultimate goal to enhance the infrastructure’s resilience. A solid base to start with is the various standards and models foreseeing different classes of threats and resilience quantities, depending on the point of view and the hierarchy of security principles, such as the NFPA 1600, ANSI/ASIS SPC.1-2009, and ISO 22301 Standards [1–3].

The issue is very important nowadays since, due to the technology advancements, the CIs are dealt as cyber-physical (CPS) systems. In this context, the telecom CIs can be regarded as fundamental, considering the large impact that wireless and data networks have on the CIs, especially in light of the emerging 5G revolution and the Internet of Things (IoT) world approaching fast. Since almost all CIs, such as energy or transport, greatly depend on telecommunications and data networks, it is clear that this interdependence will surely become more evident and profound in the near future.

The threats and resilience in telecom CIs have also been largely dealt in the literature, while specific bodies like ENISA have already made relevant classification [4]. The literature attempts are to identify and classify existing security and resilience metrics and evaluation criteria; however, the descriptions are often vague, and the evaluative factors are rather provided at a conceptual level or through a theoretical formulation. Thus, the focus of resilience metrics remains more on summative indicators rather than meaningful, risk-based ones to determine the effectiveness of a strategy [5].

Various operational organization schemes have been proposed towards that target. Nevertheless, in the majority of the literature, they are seem to be tailored to the specific infrastructure, networks, or systems needs or characteristics that the metrics are applied instead of a more generally employed approaches. And this is reasonable since each network (power grid, gas, or telecom) has its own features, procedures, and technical subsystems. It is thus recognized that crucial gaps are identified regarding the existence and evaluation of (statistically or other) sound metrics in a general manner [6].

Addressing these gaps and challenges, the ongoing RESISTO project introduces a holistic approach for the security and resilience enhancement that could be potentially implemented to serve all types of CIs. In the present work, the relevant proof of concept will be held for the telecom CIs, the significance of which is emphasized previously; these will act as the case study for the RESISTO implementation focus, paving the way for its future expansion and adaptation to other CIs such as energy and ports. RESISTO also encompasses to examine the interconnections and/or the dependencies with other critical infrastructures, presupposing their location in the vicinity of the telecom ones.

19.1.2 Security Threats and Resilience Challenges within RESISTO

Since RESISTO aims to prove a holistic approach that can be employed for all kinds of CIs, a more generic classification of threats is adopted, as following:

- Physical threats that affect physical systems, buildings, and infrastructure
- Cyber threats that exploit vulnerabilities causing possible harm in the digital realm
- And "cyber-physical" threats (combined ones) where exploited physical vulnerabilities can enable security issues in the cyber space and vice versa

The most common impression when discussing about physical security is that of dealing mainly with the protection of building sites and internal equipment from theft, vandalism, natural disasters (i.e., floods, earthquakes, fire), man-made catastrophes, and accidental damage or unintentionally destructive acts. Thus, it requires suitable emergency preparedness and appropriate safeguarding from intruders [7]. Cyber threats on the other side affect the whole operation as a software system and service, basically involving cyber intrusions, cybercrime, and deliberate malware in the CI operator's firmware, causing broader impact to the services and customers' personal data.

Physical security is often thought as only controlling personnel entrance and preventing attackers from gaining access and causing damages. However, its relation to endangering information systems is more than crucial, and it is often overlooked since most organizations focus on countermeasures to prevent hacking attacks [8, 9]. As new technologies such as biometrics and remote security become widely available, the challenges of implementing physical security are much more important now than in previous decades. Traditional card and guard security is being supplanted by identification and tracking systems in and around the facility [10]. Although cyber threats are reasonably given major attention, since data security is a primary factor, the physical ones are not evenly regarded, and physical security is often a second thought [8].

Nowadays the malicious attacks turn to be more sophisticated and aware of new technologies, imposing equally sophisticated countermeasures. Physical threats include intrusion (i.e., unauthorized access causing damages or terrorism actions), airborne and land threats (explosions, bombing by aircrafts or land vehicles, hostile drones, and unmanned aerial vehicles – UAVs – bearing weaponry), and deliberate jamming, apart from the natural hazards, affecting also the vicinity of the CI. In this context, cyber threats, apart from relative direct actions, can be also seen as a result of physical security breaches (cyber-physical threats). Organizations often focus on technical and administrative controls, and as a result, security breaches may not be discovered right away.

Cyber-physical threats include disruptions to information systems, which directly affect physical infrastructure services or intrusions to the physical domain that can cause possible harm in the CI's cyber domain. The main point when addressing and confronting cyber-physical threats is their early detection and correlation between the events. It is assumed that the cyber or physical threat events can be detected independently from the operator's corresponding security systems. However, the timely correlation between the two events is what would need a more concentrated focus to be able to detect early enough if an, i.e., physical intrusion, that would either way be detected in any case, could enable, i.e., a dormant software to the CI's cyber domain. Thus, early detection to provide alerts and intrusion events but also timely correlation between the two types of events are needed as well to improve resilience and security against sophisticated cyber-physical threats. The aim is to contribute to the overall protection concept as well as to the risk and resilience assessment of the whole infrastructure.

Resilience is the system's ability to both absorb the impact and recover rapidly from a disruption and return back to its original service levels [11]. In the context of a CI, resilience is defined as the ability of a facility or asset to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance [12]. In order to evaluate the infrastructure resilience and the effectiveness of related strategies, metrics are needed to assess and allow the decision makers to check various threat scenarios.

It is generally admitted though that it is difficult to measure resilience since it not directly observable per se but must be placed in relation to a given outcome [13]. Metrics should be specific to the contexts of the considered system, and this precludes generic indicators and thresholds; therefore benchmarks are rather difficult. A spectrum of resilience factors (for the specific system) is more meaningful, due to the dynamic and multi-dimensional nature of resilience and the fact that it is not always easy to obtain reliable, objective, and comprehensive data [13]. Attempts to derive a resilience measurement index specifically for the CIs were carried out in the USA especially after devastating natural disasters (Hurricane Katrina, 2005, and Superstorm Sandy, 2012) [14]. The methodology is based on multi-attribute utility theory, decision analysis, value patterns, and weights. However, it is noted that a relative measure is represented, while the limitations related to the subjective interpretation or use of the collected, through survey tools, data, and associated indices due to the human intervention, need to be considered.

Especially for the telecom infrastructures, apart from certain systematic approaches in recent works [15], ENISA in [4] fully recognizes similar gaps in the whole process including the lack of a standardized framework, common for all telecom providers. Although ENISA's Resilience measurement framework is meant for the existing commercial telecom networks, it addresses the issue by bringing together different taxonomies in an overall, unified, and flexible classification model, successfully addressing the weaknesses found in literature; the model includes a two-dimensional approach, incident- and domain-/discipline-based, with relevant grouping of the various metrics.

19.1.3 The RESISTO Resilience Framework

In light of the above, the ambition of RESISTO is to provide a more holistic approach. The RESISTO integrated risk and resilience management process is based on the ISO-31000 standard for risk management and formulates the Long-Term Control Loop of the RESISTO system, as it will be seen later. The complete process is being analyzed and described in detail in [16, 17] and uses suitable metrics to assess system performance and decides upon mitigation options based on the obtained information; it first identifies the system functions and derives proper resilience-related quantities that will provide the required information to facilitate the decision-making process.

Nine steps are involved, while several input tables are gathered from an extended threat list (step 1). Dedicated information for four main process steps is collected:

- System components → Step 2: System analysis
- System functions → Step 3: System performance function identification
- Threats → Step 4: Disruptions identification
- Mitigation options → Step 8: Selection of options for modifying resilience

The system performance functions (SFs) identified in step 2 constitute resilience quantities that need to be monitored, computed, or generated. In particular, they are necessary input for the pre-assessment of critical combinations of system functions and disruptions (step 5), the resilience quantification (step 6), and its final cost evaluation (step 7). For each one from the list of all SFs, obtained by the telecom CIs operators, several input fields are contained in the relevant template. An important feature of the template is the linkage between the tables, in this case the identification of system components needed for the SF to perform properly (Linked Components). This enables monitoring the propagation of the malfunctioning of a specific device (System Component) due to a disruption (Threat) to the performance loss of a specific service (System Function).

As soon as the mitigation options are finally selected (step 8), their implementation is to be held (step 9) closing the whole tool cycle. The resilience quantification is based on a computation of the performance loss due to the disruption by means of network simulations and exemplary resilience curves. Detailed results can be obtained by using the identified system performance functions, e.g., a certain failure might only affect specific services, while other functions are still working. A schematic representation of the joint risk and resilience process is shown in Fig. 19.1.

In the framework of the RESISTO project, this resilience and risk assessment management tool formulates the Long-Term Control Loop of the overall RESISTO platform that is the subject of the next section.

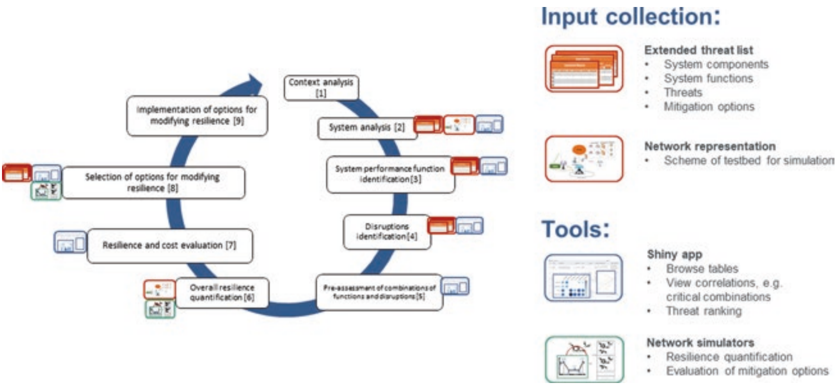
Context analysis [1]
System analysis [2]
System performance function identification[3]
Disruptions identification[4]
Pre-assessment of combinations of functions and disruptions[5]
Overall resilience quantification [6]
Resilience and cost evaluation [7]
Selection of options for modifying resilience [8]
Implementation of options for modifying resilience [9]
Input collection:
Extended threat list
• System components
• System functions
• Threats
• Mitigation options
Network representation
• Scheme of testbed for simulation
Tools:
Shiny app
• Browse tables
• View correlations, e.g. critical combinations
• Threat ranking
Network simulators
• Resilience quantification
• Evaluation of mitigation options

Fig. 19.1 Risk and resilience management process with supporting inputs and tools for the RESISTO project

The concept is proven through implementation in telecom CIs; however it can also adequately be applied to other kinds of CIs.

19.2 The RESISTO Solution

19.2.1 Concept and Approach

The RESISTO concept aims to develop a cooperation platform framework that allows different parts of the overall CI security personnel to exchange data and signals, to recognize complex attack patterns from different sources, and, based on real-time simulation of attack propagation within the CI and across interconnected CIs, to select and implement the best response and the optimal mitigation strategy. RESISTO aims to advance the infrastructure's security and resilience by developing an "entity," encompassing a holistic ecosystem of technology innovations and operational models. In fact, RESISTO takes up this challenge by fostering integrated risk-resilience assessment, faster detection of threats, better informed decision-making, and holistic understanding of a situation across the cyber and physical domain and interlinked CIs, allowing for better reaction and more efficient selection of countermeasure and mitigation actions. The logical architecture of the RESISTO platform is modular and adaptable to interfacing the existing infrastructures addressing the following five core functions, as in Fig. 19.2.

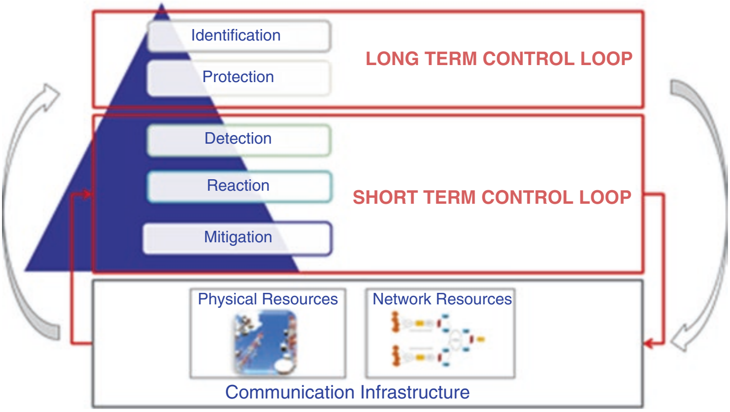

Fig. 19.2 The RESISTO logical architecture

Identification For defining and maintaining a knowledge base on physical and cyber security risks to systems, assets, data, and capabilities characterizing Telecom CIs.

Protection For developing and implementing appropriate safeguards to ensure delivery of CI services. The high degree of redundancy that usually characterizes telecommunication networks is further emphasized, in order to implement high resilience solutions. Graceful degradation of performance, when under attack, takes advantage of Network Functions Virtualization (NFV) and Software Defined Networking (SDN) paradigms.

Detection For early and timely discovering of physical and cyber security events. It includes continuous monitoring of the security status of the CI, operating in a highly dynamic environment with changing threats, vulnerabilities, technologies, business processes, and services. Key Performance Indicators (KPI) monitoring and interdependency models are further exploited to evaluate impacts, recurrent patterns, and the occurrence of complex events. RESISTO leverages on using sophisticated technologies, properly integrated with security solutions/components already available in the CI.

Reaction For orchestrating and implementing effective response to a detected event. RESISTO investigates the joint use of Security Function Virtualization (SFV) and Software Defined Security (SDS). The best response is achieved through tools for automatic impact assessment of the security risks and effectiveness of potential countermeasures.

Mitigation For developing and implementing appropriate actions to mitigate the threats' impacts and to restore as possible capabilities impaired due to security events.

19.2.2 The RESISTO Architecture and Key Elements

The platform integrates two control loops both running on top of the communication infrastructure and being interlinked with each other [18].

The Long-Term Control Loop (LTCL) is an offline procedure, following a well-defined methodology and supported by advanced tools, aiming to assess infrastructure vulnerabilities and cyber and physical threats and consequently to define assets configuration and interventions in order to improve CI resilience and robustness. For each loop cycle, a set of resilience indicators (RIs), relevant to critical threat event typologies, are estimated and stored in a knowledge base (KB). The LTCL is based on the risk and resilience assessment analysis and management process and tool, described in the previous section, which identifies and evaluates risks and suggests mitigation strategies on the CI configuration. A LTCL cycle is performed on a periodic basis or when particular events take place (new threats or discovery of previously undetected vulnerabilities).

The Short-Term Control Loop (STCL) is the runtime component of the RESISTO platform. It promptly reacts to detected cyber/physical attacks and events that may impact the operational life of the system. It enhances situation awareness and provides operators with a Decision Support System cockpit able to implement the best reactions to an identified adverse event with the aim of mitigating the event's effects and restoring standard operating conditions. The Short-Term Control Loop:

- Monitors the physical and cyber security status of the infrastructure in order to collect and/or detect anomalies, correlates the physical and cyber domain events, and provides early warnings on attacks or events adversely impacting security

- Evaluates the event impact to performance degradation of detected anomalies and attacks on the communication CI and interlinked CIs, based on cascading effects
- Supports decision-making providing a qualitative and quantitative What-If analysis tool in order to evaluate the best communication CI reconfiguration
- Drives reaction and mitigation through action workflows (as directives to intervention teams, physical protection devices activation) and, mainly, through orchestrated communication network reconfiguration and protection function activation

While the short-term loop provides tools for direct reaction against attacks in real time, the long-term loop leads to the identification of criticalities and definition of long-term strategies. The input data to the STCL and generally to the RESISTO platform include physical events (e.g., intrusions, damage) or potentially dangerous events (e.g., unauthorized UAVs); cyber-attacks; physical telecom CI monitoring data (e.g., power usage information and faults); and communication network monitoring data (e.g., traffic, alarms).

RESISTO acts complementary to the existing CI's security systems. Thus, in order to detect threat events and identify relevant hazardous data sources, it exploits and integrates various systems, both those already available and those introduced by RESISTO. The already available systems involve legacy Physical Security Information Management (PSIMs) system(s) Security Operating Centers (SOCs) or physical and cyber-attack detectors made available by the operator. Moreover, additional physical and cyber threat detectors are directly offered by RESISTO and are meant to detect more sophisticated kinds of threats as those emerging nowadays, i.e., using UAVs during malicious or terrorist attacks. The RESISTO threats detectors include airborne threats detection systems (namely, radars and acoustic sensors) for early detection against airborne threats; additional cyber threat detectors such as Open-Source Intelligence (OSINT)-based detectors; audio and visual analytics for identification and pattern recognition of physical intrusions; along with wireless devices for smart spectrum surveillance and/or blockchain functionalities acting as sensing networks in cases of intrusion through putting unauthorized devices into a telecom wireless network.

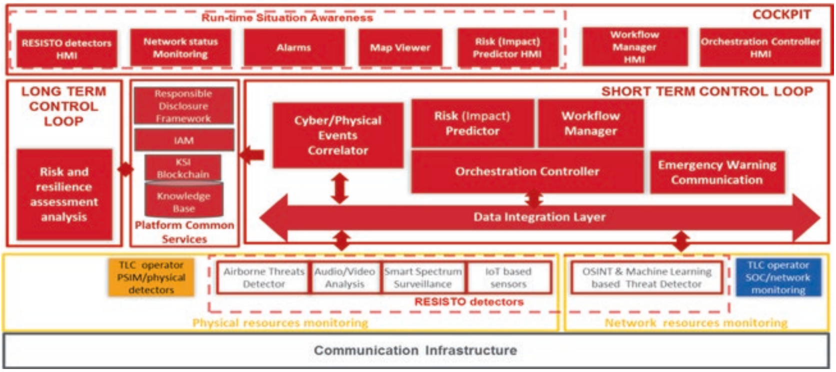
Run-time Situation Awareness
COCKPIT
RESISTO detectors HMI
Network status Monitoring
Alarms
Map Viewer
Risk (Impact) Predictor HMI
Workflow Manager HMI
Orchestration Controller HMI
LONG TERM CONTROL LOOP
Risk and resilience assessment analysis
Responsible Disclosure Framework
IAM
KSI Blockchain
Knowledge Base
Platform Common Services
SHORT TERM CONTROL LOOP
Cyber/Physical Events Correlator
Risk (Impact) Predictor
Workflow Manager
Orchestration Controller
Emergency Warning Communication
Data Integration Layer
TLC operator PSIM/physical detectors
Airborne Threats Detector
Audio/Video Analysis
Smart Spectrum Surveillance
IoT based sensors
RESISTO detectors
OSINT & Machine Learning based Threat Detector
TLC operator SOC/network monitoring
Physical resources monitoring
Network resources monitoring
Communication Infrastructure

Fig. 19.3 The RESISTO high-level architecture and key elements

The RESISTO architecture is shown in Fig. 19.3. From a functional point of view, the input data are collected by the Cyber/Physical Events Correlator, a rule-based engine applying customized rules to correlate cyber-physical threat events and to generate and propagate alarms and externally detected and collected attack/anomaly events from apparently harmless events and monitoring data. The anomalies detected by the Correlator trigger the Risk Predictor which evaluates and highlights the impacts of the detected anomaly on the communication infrastructure and, mainly, on the services provided.

In parallel, the Correlator triggers the Workflow Management software engine to guide the operator during the reaction phase. Complex actions are performed by the Orchestration Controller built around the concept of SDS, taking advantage of NFV and SDN paradigms of the underlying communication network. Finally, the Emergency Warning Communication (EWC) function is activated when there is a need for sending instant messages, targeted alerts, and operating instructions to specific users present in areas where events like natural disasters and physical or cyber-attacks are occurring.

It is seen that the RESISTO solution aims to address all possible kinds of threats along with to derive to an innovative holistic solution for the CIs, availing all resilience cycle phases (prepare, prevent, detect, respond, mitigate) and covering both immediate and long-term responses and most importantly attempting to provide the needed correlation between physical and cyber threats as well as the impact on their propagation.

19.3 Validation Cases: Analysis and Discussion

The proof of concept of the above architecture is being held through certain cyber-physical threat scenarios, described in the following, being the most representative, sophisticated, and interesting cases when considering the modern types of attacks.

In the most devious attacks, rather than trying to gain full access into the system, an attacker may only want to open up a few strategic holes to the cyber domain of a network that will cause severe problems or failures to the offered services either immediately or at a later time. In the latter case, the attackers may perform reconnaissance and preparatory work on the digital front, before moving to actually perform the attack.

Thus, the attackers can exploit vulnerabilities in the physical domain of an infrastructure, to gain access to the cyber domain. These seemingly unimportant physical intrusions (unauthorized access to a building without obvious, direct or severe damage on the infrastructure) may be initially seen as physical assaults of a lesser importance in respect to their consequences on the cyber domain; especially when correlation between the physical and cyber intrusion events is hardly performed by the operator's existing security system. Thus, both events may not be given the proper attention.

The RESISTO Use Case for Cyber-Physical Threats

A cyber-physical attack takes place, targeting network equipment in a specific location that is physically protected by the telecom provider's security system. The physical attack (either by a hostile drone or by an intruder) is performed against the physical assets of the telecom provider. This physical threat is deliberately meant to enable a security threat in the cyber domain of the telecom provider's network. The telecom facilities are protected by the provider's existing security system, while the RESISTO platform, with its additional new sensors for detection, is also deployed. Two variation scenarios are envisioned, indicating the RESISTO added value to the provider's security systems:

First Scenario In this subcase, the attackers use a UAV to overcome the physical security (i.e., secure fence protected by the telecom operator's security system) and gain access to a network switch located inside a protected building and execute a cyber-attack. The UAV flies over the fence and approaches the building, ignoring its physical security. As it approaches, it is detected by the RESISTO airborne threat detector (radar and acoustic sensors); the detection system provides information about the path followed by the UAV and issues an airborne intrusion event to the RESISTO platform.

The drone connects wirelessly to the wireless network from the exterior of the building, gaining access to the network switch, initiating, i.e., a denial of service (DoS) attack, which targets the switch. Having detected the potential airborne intrusion, the RESISTO system identifies a potential security threat in the cyber domain, marking the cyber assets in the location as "compromised." Thus, it activates various cyber detectors of the provider's network to detect possible threats in the cyber domain. Subsequently, the DoS attack is detected, and a cyber-attack event is issued by RESISTO. Finally, RESISTO suggests a prevention/mitigation action, i.e., deactivation of the switch and redirection of normal traffic, neutralizing the attack.

Second Scenario In the second subcase, an attacker/unauthorized person breaches the secure perimeter, gains physical access to a protected building, and manages to enter the facility. The keycard access system is compromised, allowing the attacker to gain access to the building. Having entered the building, the unauthorized person gains access to an unattended computer and installs dormant malware that will be activated at some point in the future.

An audio/video analytics system (as a perimeter protection functionality complementary to the existing security system of the facility) is in operation for the detection and classification of this abnormal activity. The attacker is detected using data from the provider's sensors (i.e., cameras and microphones), which are processed by the sophisticated algorithms of the RESISTO audio/video analytics sub-system and a perimeter breach event is issued to the RESISTO platform. Thus, telecommunication assets in the vicinity are identified as "compromised." The RESISTO system activates various cyber detectors in the provider's network, which eventually detect the malware. A prevention/mitigation action is suggested, and the malware is removed. A potential threat in the cyber domain of the CI has been detected and eliminated by the prevention mechanisms activated by RESISTO.

In both scenarios, the intrusions initiate an attack in the cyber domain that would potentially cause a core network failure, either immediately or at a later time. Malware (active or dormant) can initiate a DoS to a server cluster, causing network traffic or partial shut downs. This attack will have an immediate effect to telecommunication assets, systems, and the offered services, along with impacts from the operational, economic, and societal point of view. Thus, a cyber-physical attack is executed by malicious artifacts or by an attacker targeting the provider's network, and it is being detected and neutralized by the unique capabilities of the RESISTO system. These are the integration of existing and new sensors along with the advanced functionalities and the decision-making mechanisms offered by the RESISTO system.

The use case concept builds on recent trends in airborne attacks, where airborne platforms, such as drones or small aircrafts, are used to not only perform physical attacks (i.e., bombing) and/or gather intelligence for physical security vulnerabilities but also gain access and compromise the cyber domain of the CI, directly attacking it, i.e., by connecting to the wireless network of a facility. This way, these scenarios represent realistic cyber-physical attacks that would perfectly fit an urban environment, where drones or UAVs are used for commercial purposes and can be concealed behind everyday activity that would not raise any kind of suspicion.

Both subcases cannot be detected and mitigated efficiently by conventional security systems. Although separate physical and cyber security mechanisms may be in place, the correlation between the events identified by RESISTO facilitates the efficient detection of the attack and enables its mitigation in its entirety. As it seems although both the physical location and the network were already protected by the physical and cyber detectors of the provider, without the RESISTO platform, the threats would not even be detected, let alone neutralized. Table 19.1 provides a summary of all response steps of the RESISTO solution.

19.4 Conclusions

The main objective of the RESISTO platform and the respective use cases is to enhance the resilience of the existing communication CIs toward both the domains of physical security and cyber protection. The focus is to advance the processes of detection and response and to result in new additional measures for mitigation and prevention, confronting threats that would have not been identified without the RESISTO system. It is

Table 19.1 The RESISTO response

Sequence	*Action steps – analysis*
Detection	Physical threats detected by the RESISTO sensing systems and legacy ones.
Reaction	*Correlation*: of the cyber-physical threat events, based on the RESISTO STCL correlation engines rules *Identification*: of the cyber assets in the location as "compromised" The STCL initiates various cyber detectors to detect the cyber malware. *Issue of event*: a cyber-attack event is issued by RESISTO *Countermeasures*: triggered by RESISTO, i.e., providing emergency signals *Notifications*: notifying the security operation center or the decision-making
Mitigation/ prevention	RESISTO STCL suggests deactivation of the switch and redirection of normal traffic (traffic rerouting). The malware is removed from the network *RESISTO LTCL iterations*: proposes disaster recovery plan (best practices and/or redundancy/resilience centers in respect to the assets affected)
End of cycle	RESISTO ensures communication continuity in the end

considered that a physical intrusion in a telecom operator's infrastructure can facilitate severe assaults in the cyber domain of a telecom network and vice versa. The main challenge is to perform this correlation in the short term and activate the respective response and mitigation actions; thus to prove that it is possible to detect the consequences of combined threats in short time and to use joint countermeasures.

It should be pointed out that these kinds of threats are not possible to be detected, correlated, and identified by the conventional security systems already used; instead they would be identified separately as only physical or only cyber ones, respectively. In such case, they would constantly cause security impacts requiring much more time and costs before they are finally identified and confronted, since the core of their creation would have remained undetected. RESISTO performs this correlation feature, enabled by additional sensors and algorithm framework, facilitating an effective detection of the attacks along with decision-making mechanisms for their response and mitigation.

The RESISTO proof of concept is being implemented to communication CIs. However, the fact that RESISTO can act complementary to conventional security systems and since other CIs greatly depend on telecom services (i.e., cyber domain or cloud data), it is evident that the above analysis can be adequately applied also in other kinds of critical infrastructures with similar implementation.

Acknowledgments This work is supported by the EU-H2020 RESISTO project, which has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No. 786409 (http://www.resistoproject.eu/).

References

1. NFPA. (2010). NFPA 1600-Standard on disaster/emergency management and business continuity programs, MA, USA, 52 p. .http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf
2. ASIS, The Organizational Resilience Standard [ASIS SPC.1-2009]. (2009). Available at http://organizational-resilience.com/OrganizationalResilienceStandard.htm
3. ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements. (2012). Available at http://www.iso.org/iso/catalogue_detail?csnumber=50038
4. European Network and Information Security Agency (ENISA). (2011, February). Measurement frameworks and metrics for resilient networks and services – technical report.
5. Hayes, B., & Kotwica, K. (2012). Advances and stalemates in security. *Security Magazine, 34.*
6. Ohlhausen, P, et al. (2014). Effective, evaluated security metrics – persuading senior management with effective, evaluated security metrics. ASIS Foundation Report.
7. IES/NCES, National Center for Education Statistics, US Department of Education. https://nces.ed.gov/pubs98/safetech/chapter5.asp. Last accessed 2019/11/2.
8. Harris, S. (2013). Physical and environmental security. In *CISSP exam guide* (6th ed., pp. 427–502). New York: McGraw-Hill.
9. Hutter, D. (2016). *Physical security and why it is important*. GIAC (GSEC), SANS Institute. https://www.sans.org/reading-room/.../physical/physical-security-important-37120.
10. Niles, S. (2015). Physical security in mission critical facilities. White Paper 82, revision 2, APC White Papers, Schneider Electric's Science Center.
11. Omer, M., et al. (2009). Measuring the resilience of the trans-oceanic telecommunication cable system. *IEEE Systems Journal, 3*(3), 295–303.
12. Carlson, J. L., et al. (2012). *Resilience theory and applications*. Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL, USA.

13. Food Security Information Network. (2016). Measuring resilience. Crown Copyright. https://doi.org/10.12774/eod_tg.may2016.sturgess2.
14. Argonne National Laboratory. (2013, April). Resilience measurement index – an indicator of critical infrastructures resilience. ANL/DIS-13-01 Report, US Department of Energy.
15. Smith, P., et al. (2011, July). Network resilience: A systematic approach. Topics in network and service management. *IEEE Communications Magazine*, 88–97.
16. Häring, I., et al. (2017). Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. In I. Linkov and J. M. Palma-Oliveira (Eds.), *Resilience and risk (NATO SfP and Security Series C: Environmental Security)* (pp 21–80). Dordrecht: Springer Netherlands.
17. Fehling-Kaschek, M., et al. (2019). A systematic tabular approach for risk and resilience assessment and improvement in the telecommunication industry. In *Proceedings of ESREL 2019 Hannover* (pp. 1312–1319). Singapore: Research Publishing.
18. The RESISTO Consortium: D2.6_RESISTO platform and tools reference architecture deliverable. http://www.resistoproject.eu/resources/. Last accessed 2018/10/11.