PRAETORIAN: A Framework for the Protection of Critical Infrastructures from advanced Combined Cyber and Physical Threats

Lazaros Papadopoulos, Antonios Karteris, Dimitrios Soudris
{lpapadop,akarteris,dsoudris}@microlab.ntua.gr
National Technical University of Athens, Greece

Eva Muñoz-Navarro, Juan José Hernández-Montesinos
{emunoz,jhernandez}.etraid@grupoetra.com
ETRA Investigación y Desarrollo, Spain

Stephane Paul, Nicolas Museux
{stephane.paul,nicolas.museux}@thalesgroup.com
THALES Research and Technology, France

Sandra König, Manuel Egger, Stefan Schauer
{sandra.koenig,manuel.egger,stefan.schauer}@ait.ac.at
Austrian Institute of Technology

Javier Hingant Gómez
jahingme@upvnet.upv.es
Universitat Politècnica de València, Spain

Tamara Hadjina
tamara.hadjina@koncar.hr
Koncar Digital, Croatia

ABSTRACT

Combined cyber and physical attacks on Critical Infrastructures have disastrous consequences on economies and in social well-being. Protection and resilience of CIs under combined attacks is challenging due to their complexity, reliance on ICT systems and the interdependences between different types of CIs. The PRAETORIAN framework was designed to address these challenges, by integrating components responsible for detecting both cyber and physical threats. Additionally, it forecasts how the combined attacks will evolve and their cascading effects on interdependent CIs. The PRAETORIAN framework was demonstrated based on a realistic scenario in the Zagreb airport, combining both physical and cyber attacks.

CCS CONCEPTS

• **Security and privacy** → **Intrusion/anomaly detection and malware mitigation**; **Systems security**.

KEYWORDS

Physical threats, Cyber threats, Critical Infrastructure Protection, Decision Support System, Security

ACM Reference Format:
Lazaros Papadopoulos, Antonios Karteris, Dimitrios Soudris, Eva Muñoz-Navarro,, Juan José Hernández-Montesinos, Stephane Paul, Nicolas Museux, Sandra König, Manuel Egger, Stefan Schauer, Javier Hingant Gómez, and Tamara Hadjina. 2023. PRAETORIAN: A Framework for the Protection of Critical Infrastructures from advanced Combined Cyber and Physical Threats. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3600160.3605030

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605030

1 INTRODUCTION

Combined cyber and physical attacks on Critical Infrastructures (CIs) have major impact, not only on the owners and operators of these CIs, but also on their customers and suppliers. People in the vicinity of the attacked CIs, as well as neighboring and interrelated CIs are also affected, leading to widespread and often massive damages in various sectors of the economy and in social well-being.

There are many reasons why combined cyber and physical attacks on CIs are expected to become more common. To mention just a few, there is a proliferation of industrial control system malware, while there is an increased reliance of the industry and CIs on ICT systems. Additionally, the industrial control system networks are notoriously difficult to secure, while the cyber criminals have a proven business model. The impact of a coordinated physical attack, a deliberate (cyber) disruption of critical automation systems, a natural hazard or even a combined scenario including several kinds of attacks, can have disastrous consequences for the economy and social well-being in general.

Therefore, there is a need of methodologies and tools that meet the expectation needs of the CI operators in addressing the security challenges of combined attacks. These tools should extend the capabilities of the typical legacy security systems for detecting various types of threats and enable successful coordinated response to attacks. Also, they should be effective against combined attacks including both physical and cyber threats. Finally, since no CI exists and operates in isolation, the cascading effects of an attack on a single CI to others should be identified and addressed. There are several state-of-the-art frameworks which are designed to support CI operators in the anticipation and the mitigation of a combined physical and cyber attack. However, most of them are tailored to specific types of CIs, such as healthcare [1], transportation [8][2], or telecommunications [3].

The PRAETORIAN framework was designed to address the above challenges [9]. It was developed in the context of the PRAETORIAN H2020 EU funded project. The framework targets CI operators and it is an integrated toolset that allows a cooperative communication and effective preventive and mitigation actions among interrelated CIs, before and during emergencies. In contrast to other frameworks, PRAETORIAN was designed to be more flexible and scalable, with features that allow it to be adapted to different types of CIs.

This paper is an overview of the PRAETORIAN system and describes each PRAETORIAN component and the data flow between them. Also, it explains how each component can be used by the operator and its added value in the detection and mitigation of combined (i.e. cyber and physical) attacks.

The rest of the paper is organized as follows: Section 2 describes each PRAETORIAN component: The cyber, the physical, the hybrid situation awareness and the coordinated response. Section 3 explains how the PRAETORIAN was demonstrated in a realistic scenario, combining cyber and physical attacks in an airport and in a medical laboratory. Finally, in Section 4 we draw conclusions.

2 THE PRAETORIAN FRAMEWORK

Figure 1, shows the main components of the PRAETORIAN framework:

- The *Physical Situation Awareness system (PSA)* receives and processes information from sensors and other IoT devices, such as object tracking devices and UAVs and generates alarms when intrusion or hostile activity is detected at the physical domain of a CI.
- The *Cyber Situation Awareness system (CSA)* is responsible for detecting threats in the cyber domain of the CIs. It relies on novel tools, such a the cyber forecaster engine, which complement existing well-established cyber-security technologies.
- The *Hybrid Situation Awareness system (HSA)* that analyzes events, predicts how attacks will evolve and calculates the cascading effects of attacks within the same and between different CIs.
- The *Coordinated Response system (CR)* that integrates information from all other components, generates security incidents which trigger relevant notifications and recommends mitigation actions. Finally, it integrates various tools to further support effective response, enable efficient information sharing with first responders, increase situation awareness based on social media and support the interaction with drone neutralization systems.

Figure 1, highlights the flow of information between the aforementioned components. The HSA receives *events* and *alerts* generated by the PSA and CSA. The CR receives alerts from all components and generates relevant security *incidents* and proper notifications to operators and first responders, while it recommends mitigation actions.

The PRAETORIAN framework back-end is based on the *InterOperability Platform* (IOP), a database in which the generated data are stored and retrieved. It serves as a data sharing infrastructure for all PRAETORIAN components. It offers a variety of connectivity methods, including a RESTful Application Programming Interface (API), the Datagram Delivery Protocol (DDP) [4] and the Advanced Message Queuing Protocol (AMQP) [6]. About the front-end, the main PRAETORIAN HMI is the CR. However, each component (i.e. PSA, CSA and HSA) provides a user-friendly HMI, tailored to the needs of CI operators.

The following subsections are a detailed description of each PRAETORIAN component, focusing on the features and the added value that each one provides compared to the typical legacy systems.

2.1 Physical Situation Awareness

The role of the Physical Situation Awareness system (PSA) is to collect and display information gathered from the physical domain and particularly from various sensors installed in the area of the CI under study.

The PSA stores and retrieves data from the IOP through the DDP. The main front-end is the PSA HMI, which consists of the following sections:

- Map, which is the central PSA HMI and shows the earth globe with the different items (assets, agents, etc.) placed on it (Figure 2). It provides many features which allow CI operators to improve situation awareness with regard to the physical domain of CIs.
- Scenes, which are used to define the areas of CIs on the map.
- Cameras, which allows to watch and manage the camera streams.
- Chat, (i.e. a chat application integrated in the PSA), which enables bidirectional communication between different teams, as well as the exchange of files, such as videos.

Figure 2 shows an example of the PSA map view, for a port CI. Sensors in the area of the port are represented as icons on the map. They are green by default. However, they can be configured so that their color changes depending on the measured value. As an example, a sound sensor may change color when the sound of a drone is detected. (This is the case for the sound sensor, which has turned into orange color in Figure 2).

CI operators can watch on the PSA HMI sensor real-time measurements and video streams. Unmanned vehicles are also visible on the map. They are shown as 3D models and they leave a trail on the map when they move. Additionally, the PSA integrates the IDEMIA Augmented Vision Platform [5]. Examples of its capabilities are the automatic detection of potential physical threats, such as intrusion detection, suspicious behavior, as well as face recognition and object classification.

The PSA map HMI displays ongoing security incidents. In the context of PRAETORIAN, the incidents are defined as events which may require immediate action by CI Operators (e.g. smoke/fire or unauthorized drone detection). By clicking on an incident located on the map, operators can view details. For example, when the incident is the detection of an unauthorized drone, clicking on it will show the live video stream of the camera that has detected it.

Finally, the PSA supports the creation of Emergency Population Warning System (EPWS) EU alerts. Operators can select an area around the incident. After selecting a message from existing templates, the operator can potentially edit the message and send it to the cell phones of the population in the area. As shown in Figure 3, a colored grid on the map indicates the number of cell phones in

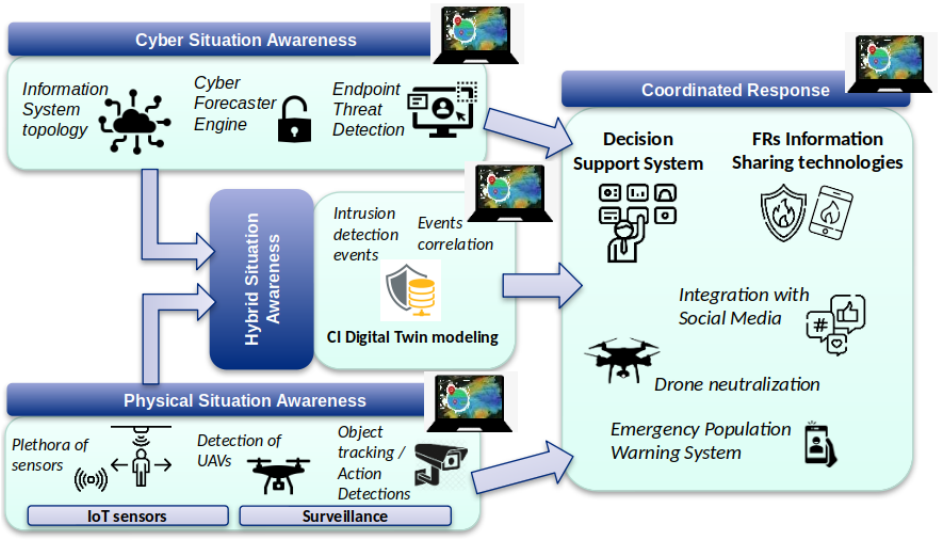

Figure 1: Overview of the PRAETORIAN framework

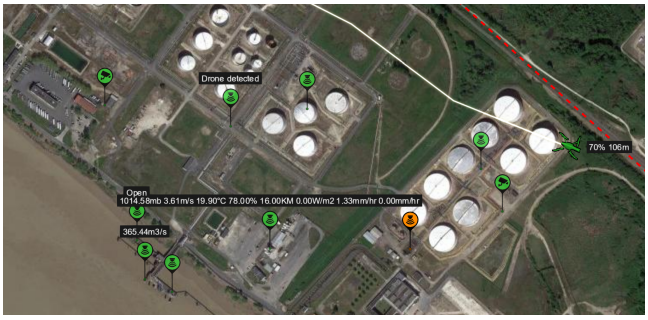

Figure 2: An instance of the PSA map view. The monitored values of each sensor are shown in real-time.

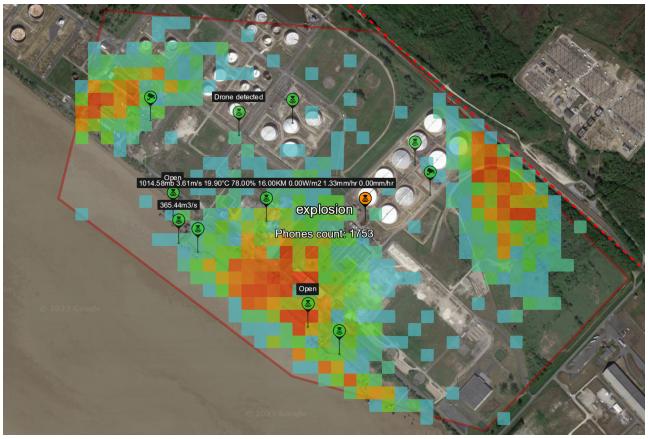

Figure 3: An example of an EPWS alert sent through the PRAETORIAN PSA

the area, which can be used to provide a rough estimation of the number of people and their distribution in the area of he incident.

2.2 Cyber Situation Awareness

The main goals of the CSA component are (i) to improve the cyber situation awareness of the CI operator and (ii) to forward cyber events to the HSA and enable their correlation with the physical events for the prediction of cascading effects.

The CSA was designed to address limitations of existing Security Information and Event Management (SIEM) tools. The main innovative element of the CSA is its forecasting features. In particular, it is capable of forecasting the end goal of an attacker based on the first detected activities of the attacker.

For this purpose, the CSA relies on Digital Twins and simulators mimicking the cyber domain of CIs, on Cyber Assessment Tools (CAT) to simulate additional legitimate traffic, launch attacks and collect cybersecurity logs and on the Cyber Forecaster Engine (CFE) to forecast the end goal of the attacker.

The CFE addresses shortcomings of cybersecurity sensors and SIEM tools, such as the fact that the SIEM tools rely only on CI-agnostic Indicators of Compromise (IoC), without any relation to business or operational impact. Thus, they lead to either false-positive cyber alarms or to late cyber-security incident generation. Additionally, stealth Advanced Persistent Threats (APT), which are developed over weeks or months, they may be detected only too late, due to lack of information transmission between operators working on different shifts.

The CFE addresses these limitations as follows: It relies on CI-specific IoCs, which are based on a risk assessment report for the particular CI. Additionally, it stores cyber events in memory, without time limitations, as long as they are valid. An event-pattern recognition engine (ERE) uses these observables and based on a set of rules recognises the attack activities. A Hypothetical Reasoning Engine (HRE) predicts the possible next steps of the attacker,

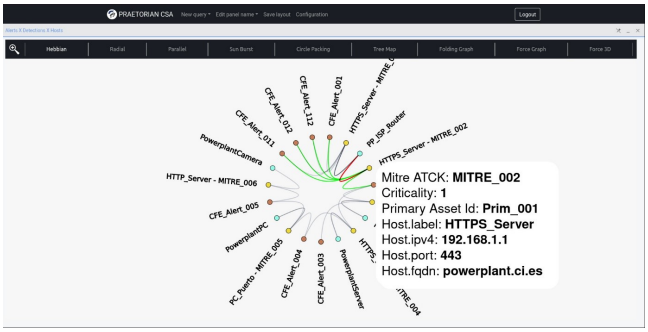

Figure 4: An example of the CSA HMI. Assets, detections, alerts and attack goals are shown with different colors.

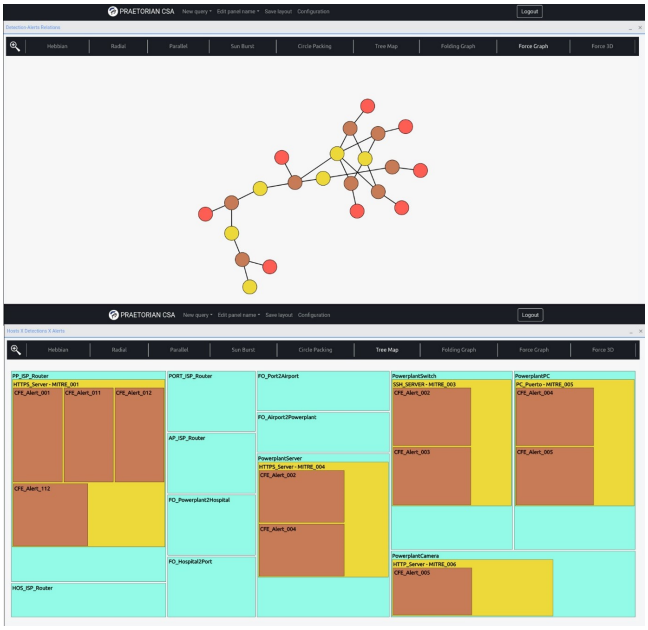

Figure 5: Alternative CSA representations. Different color is used to distinguish between the primary and secondary assets, as well as about the end goal of the attacker.

generates alerts based on the risk assessment report and provides explainable predictions to the CI operators. These alerts are forwarded to the HSA and CR for calculating cascading effects, generating security incidents, notifications and recommend mitigation actions.

The CSA HMI provides various visualization options to represent assets, alarms, detections and attack goals, as predicted by the CFE. An example is shown in Figure 4. Other visualizations, include tree map, radial, force graph, etc. Some examples are shown in Figure 5. Additionally, it provides a timeline representation of attacks, showing the relation between the detections and the corresponding alerts.

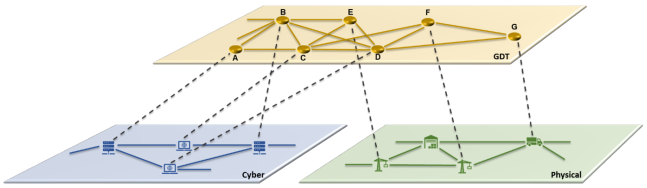

Figure 6: Schematic illustration of the overall concept of the Generic Digital Twin

2.3 Hybrid Situation Awareness

The main of the PRAETORIAN Hybrid Situation Awareness (HSA) component is to provide to CI operators accurate forecasts of potential cyber and physical consequences at the facilities, given any kind of physical and cyber alert detected by the PSA and the CSA respectively. It calculates the cascading effects of attacks on CIs, both within the particular CI, as well as on interrelated CIs.

Its main components of the HSA the following:

- A Generic Digital Twin (GDT)
- A Threat Propagation Engine (TPE)
- The Hybrid Situation Awareness HMI

The GDT is an abstract representation of the entire network of CIs. It includes the cyber and the physical digital twin of the CI , but also inter-domain knowledge. Figure 6 shows how information from the physical and the cyber digital twins is incorporated in the GDT. It can be observed that not every physical or cyber asset or every characteristic of each asset is represented in the GDT. Instead, the GDT includes the most relevant ones, as well as the ones that describe similar concepts among different types of CIs. Thus, the GDT adapts to the specific characteristics of the different types of CIs and their internal and external interdependencies, in order to be able to model the operational states of every critical asset. Dependencies between cyber and physical components are added where relevant for the analysis, e.g., encrypted data is connected to a server.

The GDT consists of a graph-based representation. The nodes represent the critical entities of the CIs, as modelled in the individual digital twins and the edges represent the dependencies among these assets. Each asset has a state, representing (i) Functionality (normal, reduced, not working) (ii) Availability (normal, interrupted, not available) or (iii) Damage (no, some, failure), depending on the type of asset.

The granularity of the models is configurable: Models can be created within a CI, to calculate cascading effects between assets of the particular CI, as well as between different CIs, for calculating the cascading effects between them. Also, the system can be decentralized or centralized: For example, in some countries 112 may act as a central authority, which may be responsible to inform the affected CIs, about, for example, calculated cascading effects. Depending on protocols and legislation, in other cases maybe one CI can directly inform another CI about cascading effects of ongoing incidents.

The state may change due to a cyber or physical event, as detected by the PSA or the CSA, respectively (e.g., fire, cyber-attack etc.). When the state of a node changes, a notification is sent to

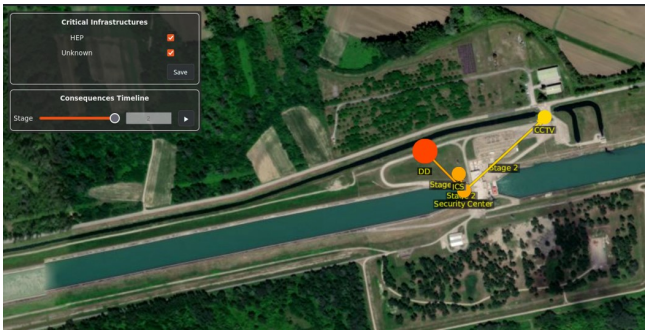

Figure 7: An example of TPE output, as displayed on the HSA HMI. The different colors indicate the state of each asset or CI. (i.e. the degree by which it is affected).

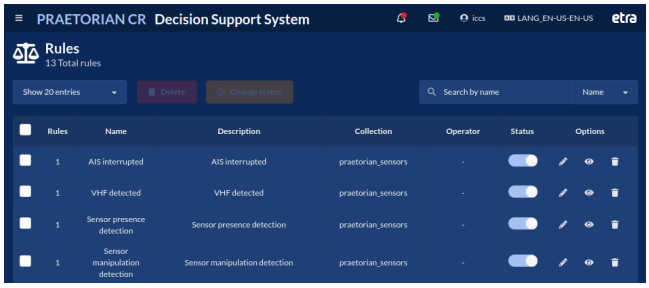

Figure 8: The rules interface of the DSS. The rules determine under which condition an event generated in the PSA, CSA or HSA will trigger the generation of a security incident. Additionally, they determine when the DSS will trigger another module (e.g. the drone neutralization module, when an "unauthorized drone detected" type of incident is created).

Figure 9: A tool for security threat detection in social media. The text of the post is displayed. The keywords and the crawling rules are highlighted with red and yellow color, respectively, to provide explainable identifications.

each adjacent node. Then, the adjacent nodes may themselves react to the incoming notification. They may change their state, and, in turn, inform their own adjacent nodes. Thus, the GDT models the cascading effects within a CI and between different interconnected CIs.

Based on the GDT, the Threat Propagation Engine (TPE) describes the direct and indirect consequences of alerts generated by the PSA and the CSA, over time. In particular, for each alert forwarded to the HSA, the TPE is triggered and a set of interdependent threat propagation simulations is run. The simulation results are used to estimate the potential consequences of the threat on the overall network of interconnected CIs. The output of the TPE is a prediction of the propagation of the cascading effects, which is displayed on the HSA HMI.

The HSA HMI displays on a map the predicted cascading effects, as calculated by the TPE simulations, on a map (Figure 7). A graph-based representation is used, in which each node corresponds to a cyber or physical asset of a CI and each link corresponds to an interdependency. Different colors in each node indicate the corresponding impact of the threat (i.e., the degree by which the asset was affected). Other features of the HMI include historical information of simulations for past alerts, filtering options, and step-by-step display of the simulation results.

2.4 Coordinated Response

The main CR module is the Decision Support System (DSS). It acts as a hub, as it collects all alerts and events generated by the PSA, CSA and HSA. Through a set of predefined *rules*, a sample of which can be seen in figure 8, the DSS generates *events* (i.e. information potentially useful to operators) and security *incidents* (i.e. information that may require immediate action by operators). Once an incident is created, responsible operators can be notified in a variety of ways, including email, SMS or through a chat application, all of which are configurable through the *notifiers* page of the DSS. Finally, in order to assist the operators in taking the appropriate actions once an incident is generated, the DSS offers a configurable list of recommended mitigation actions that the CI operator can take. The mitigation actions proposed by the PRAETORIAN DSS were obtained through interviews with the CI security operators.

Aside from the DSS, the PRAETORIAN system provides more options for the effective communication between operators and first responders, through the *Information Sharing & Communication with FRs* (ISC-FR) module. It relies on the theoretical concept of of *attribute trees* in order to gather all of the information available on the PRAETORIAN platform and discern the parts that are relevant for each type of first responder, for a particular incident type. Subsequently, the module uses the chat application as a channel for bidirectional communication. More details about the ISC-FR module can be found in [7].

Finally, the CR system offers connectivity with Twitter through the *Social Media Security Threat Detection* (SMSTD) and *Integration with Social Media* (IWSM) modules. The SMSTD utilizes text crawling techniques in order to monitor the entirety of the global Twitter stream and discern tweets that are potentially critical to the security of the CI, including tweets that mention data leaks, new vulnerabilities and cyber attacks. A screenshot with an identified tweet indicating a security threat is shown in Figure 9. The module is customizable to the requirements of type of CI, as it prioratizes posts which are potentially more relevant to the particular CI. The latter module (IWSM) offers a number of tweet templates that allow the CI operators to generate messages for the public and share them on the social media platform with the press of a button. Finally, a third module provides a real-time feed of Twitter posts by the public during a crisis. The tool relies on machine learning techniques and identifies relevant informative-only tweets which can enhance the

Table 1: Summary of demonstration scenario execution

Step		Tools involved
1	An intruder enters the medical laboratory and steals a sample.	The operators gets notified about the intrusion incident in the DSS The video analysis platform of the PSA detects the intruder
		The operator is notified about the cascading effects in the DSS HSA: The operator sees the cascading effects about other CIs affected and authorities involved
2	A cyber attack at the laboratory with a malware	DSS: A cyber incident is created and the operator gets notified CSA: The operator sees the cyber detections and alerts, the primary assets affected and the final goal of the attacker
3	A terrorist attacks the airport with a drone	DSS: The operator is notified about the drone and the DSS triggers its neutralization PSA: Sees the location on the map in real time
4	Informing the public	EPWS: The airport operator sends EU alerts Integration with social media: The operators posts a message on Twitter about the incident.
5	Involvenent of First Responders	ISC-FR: The operator dispatches to FRs information including the location of the neutralized drone, the estimation of number of people in the area (provided by the EPWS). The communication channel is a chat session: A group including the operator and First Rsponders to enable bidirectional communication

operator situational awareness during crisis. More details about this module can be found in [7].

3 DEMONSTRATION

The first pilot demonstration of the PRAETORIAN system took place at the Zagreb airport in Croatia. It was based in a cross-border scenario involving both the Medical University of Graz in Austria and the airport of Zagreb. The scenario was based on a physical and cyber attack involving bio-terrorism and drone attacks. Around 100 people joined the event either in-person or online. The video recording of the demonstration is available on the PRAETORIAN YouTube channel [1]. During the live demo, all the PRAETORIAN framework components were used by operators of both the laboratory and the airport.

Table 1 summarizes the steps of the demonstration scenario, and describes how the operators use the PRAETORIAN tools to address the attack. In particular, the attack consists of an intrusion in the laboratory of the Medical University of Graz, followed by a cyber attack. Then, the terrorist performs an attack at the Zagreb airport using a drone armed with a bio-weapon created by the stolen sample. The PRAETORIAN system can is used in this scenario (i) to detect the intrusion and predict its cascading effects (ii) to detect the cyber attack and calculate the final goal of the attacker (iii) to detect the drone and trigger its neutralization (iv) to alert the population in various ways and (v) to communicate with the first responders (the Croatian Mountain Rescue Service, in this particular scenario).

4 CONCLUSIONS

The PRAETORIAN framework is a significant contribution into addressing the challenges of CI protection from combined cyber and physical attacks. It provides an advanced toolset which can be customized to the requirements of each particular type of CI. It focuses a lot on the prediction of the cascading effects of attacks and on the impact of these effects on interdepended CIs. Finally, it provides user-friendly interfaces for effective use by the CI operators.

[1] https://www.youtube.com/watch?v=dBsY-emLehw

ACKNOWLEDGMENTS

This work has received funding by the EU H2020 research and innovation programme under grant agreement No 101021274. (PRAETORIAN, https://praetorian-h2020.eu/).

REFERENCES

[1] Elisabetta Biasin. 2020. Healthcare critical infrastructures protection and cybersecurity in the EU: regulatory challenges and opportunities. In *Proceedings of the 1st European Cluster for Securing Critical Infrastructures (ECSCI) Virtual Workshop.*
[2] Marie-Hélène BONNEAU, Laura PETERSEN, Grigore HAVARNEANU, and Stephen Crabbe. 2022. SAFETY4RAILS EU project: Protecting railway and metro infrastructure against combined cyber-physical attacks. In *World Congress on Railway Research (WCRR) 2022.*
[3] Mirjam Fehling-Kaschek, Katja Faist, Natalie Miller, Jörg Finger, Ivo Häring, Marco Carli, Federica Battisti, Rodoula Makri, Giuseppe Celozzi, Giuseppe Amato, et al. 2019. A systematic tabular approach for risk and resilience assessment and Improvement in the telecommunication industry. In *Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019). ESREL. Hannover, Germany.* 22–26.
[4] Karen Frisa and Steven Waldbusser. 1995. AppleTalk Management Information Base II. RFC 1742. https://doi.org/10.17487/RFC1742
[5] IDEMIA. 2021. Augmented Vision Platform. https://www.idemia.com/wp-content/uploads/2021/01/augmented-vision-platform-idemia-brochure-202102.pdf
[6] ISO/IEC 19464:2014 2014. *Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification.* Standard. International Organization for Standardization, Geneva, CH.
[7] Antonios Karteris, Georgios Tzanos, Lazaros Papadopoulos, Konstantinos Demestichas, Dimitrios Soudris, Juliette Pauline Philibert, and Carlos López Gómez. 2022. A Methodology for enhancing Emergency Situational Awareness through Social Media. In *Proceedings of the 17th International Conference on Availability, Reliability and Security.* 1–7.
[8] Corinna Köpke, Louis König, Katja Faist, Mirjam Fehling-Kaschek, Jörg Finger, Alexander Stolz, Kelly Burke, Eftichia Georgiou, Vasiliki Mantzana, I Chosiotis, et al. [n. d.]. Security and resilience for airport infrastructure. In *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference.* 1191–1198.
[9] PRAETORIAN. 2021. Horizon2020 Project. https://praetorian-h2020.eu/