Professional paper

Crisis Management and Resilience of Critical Infrastructure: SUNRISE Project Insights

Aljosa Pasic[1]

[1]Atos Spain, aljosa.pasic@atos.net

Abstract: *Crisis management is often considered as the short-term, reactive strategy to handle emergencies, while critical infrastructure resilience is a long-term, proactive approach to reduce vulnerabilities and enhance stability. SUNRISE (Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe) is a project, co-funded by the European Commission, that considers lessons learned from COVID-19 pandemics, as well as the related challenges for critical infrastructures (CI) operators to come up with solutions that would help in improving their resilience. This paper explains the main project concepts and brings some insights about how to handle temporary operational conditions during unexpected rapid-onset events.*

Keywords: *resilience, critical infrastructure, EU projects*

1. INTRODUCTION

Resilience is a concept that spans different domains (physical, information, cognitive or social) and has different capacities, abilities, or principles in face of different adverse events. These events can be categorized as slow-onset or rapid-onset based on how quickly they manifest and escalate. Climate change, geopolitical tensions or rising unemployment can be considered as a slow-onset events. Natural disasters, stock market crash, or power grid failures are examples of rapid-onset events. Event such as pandemic falls into both categories. It might initially spread slowly before reaching global impact, but there could be transitions to rapid-onset event during a critical period. Understanding this dual nature is therefore crucial for effective pandemic preparedness and response strategies. Healthcare systems, or critical infrastructures in general can experience near-instant service degradation due to a surge in cases, causing a rapid shift from containment to crisis management.

In this context, we can also mention many EU efforts, starting from the European programme for critical infrastructure protection (Council Directive, 2008), which establishes a procedure for identifying and designating European CI, to a more recent Directive on the Resilience of Critical Entities (CER Directive, 2022) that entered into force on 16 January 2023. In contrast to the previous approach, with more focus on prevention and mitigation, CER directive also focuses on the response and the rapidity of recovery during and after the event.

SUNRISE (Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe) is a project, co-funded by the European Commission, that considers lessons learned from COVID-19 pandemics, as well as the related challenges for critical infrastructures (CI) operators to come up with solutions that would help

in improving their resilience. Project approach is user-driven with national, as well as the cross-country workshops conducted in a systematic manner to shape challenges and requirements for the design of the system.

This paper explains the main project concepts and brings them in relation to crisis management process that involves identifying potential crises, preparing for them, responding to them, and mitigating their potential damages. Organizations and government entities must be prepared to handle sudden crises, linked to unexpected rapid-onset events that occur without warning, as well as other types of crises, such as those caused by the failure to respond effectively to early warning signs, including health crises, cybersecurity breaches, or critical infrastructure failures. The SUNRISE objectives are addressing both strategic level with scenario-based planning and simulation tools, as well as awareness of the dynamic threat landscape related to and implied by pandemics, often observed at the operational level, where several technological solutions have been implemented. While resilient infrastructure reduces the severity of crises, making crisis management efforts more effective, specific activities during crisis management, such as rapid anomaly detection in infrastructures, can support continued operation or quick restoration of critical infrastructures. Concepts related to structured response based on observation and orientation are also explained in scenarios which include “threat multipliers”. Finally, the use of artificial intelligence technologies in SUNRISE, for example in demand prediction or in anomaly detection, are also briefly explained in this paper.

2. METHODOLOGY

The current critical infrastructures (CI) and supporting information systems have evolved into a highly distributed infrastructure, crossing several domains, such as energy, transport, healthcare, or finance. This complexity, and relatively poor collaboration and data sharing between CI domains, makes them increasingly vulnerable.

When it comes to diversity of CI operators, types of assets are different in each sector, so that impacts and consequences can be different (e.g., availability of CI might have large consequences on the overall economy). In SUNRISE we used both:

- Deductive methods: from generically applicable strategy for the main pandemic risks, to the sector and user specific scenarios that include some combination of “threat multipliers” (e.g. cybersecurity attack during pandemics), “derived risks” (e.g. restrictions of movement due to the lockdown) or “contextual changes” (e.g. changes of priority or supply chain). Scenario planning, macroeconomic risk assessment, simulation of cascading effects and “what-if” analysis were all developed and validated by strategy implementation organizations (including national and regional authorities).
- Inductive methods: from specific cases to some generic conclusions, for example how implementation of some technologies or procedures in a specific CI operator might influence infections among essential employees. The best example is when operators faced a spike in phishing and ransomware attacks, expecting therefore that all critical infrastructure could expect similar attacks and should therefore enhance threat intelligence sharing and detection based on similar patterns

Initial material to address needs and derive requirements was collected during the workshops with CI operators that were held in Spain, Slovenia, and Italy. The Spanish workshop, for

example, was held on 9th of May 2023 at the Universidad Politécnica de Madrid (UPM), in Madrid, Spain. It was led by UPM, who is the Spanish cluster lead, with the support of Atos (ATS), who is the vice-leader of the Spanish cluster. All the Spanish Critical Infrastructure (CI) operators participating in SUNRISE, including Acosol (ACO, water sector), Quirón Salud and Hospital Quirón Madrid (QS/HQM, healthcare sector), Consorcio Regional de Transportes Públicos Regulares de Madrid (RTM, transport sector), and Telefónica (TLF, telecommunications sector) and the Spanish CI supervisory authority (MIR, Ministerio del Interior) participated in the workshop. Additionally, there were actors from the Banking sector, Energy sector, Industrial Association, and Health Authorities. Final user requirements collected from CI operators for cyber resilience use case were reported in SUNRISE deliverables, with a special emphasis on two specific use cases from Italian public administration and water management CI operators. In case of each type of technological solution, additional in-depth interviews were held. For example, in case of cybersecurity, interviews with these two CI operators were done during the spring of 2024, where many cybersecurity contextual inputs were collected, with a specific focus on temporary operational conditions (e.g. procedures or percentage of remote workers), threat modelling, as well as organizational cybersecurity risk models.

Demand of critical goods to ensure business continuity or uncertain availability of skilled workers are examples of pandemic specific risk indicators to be considered across all sectors, while human risk indicators are not limited only to the absenteeism, but also related to training and awareness, psychological or behavioral risks, including trust, urgency, fear, greed, helpfulness, or curiosity. Pandemic event also brings supply chain risks, imbalance in the workload, weak coordination, parallel decision making, lack of integrated health protocols, etc. Besides SUNRISE strategic framework, supported by a specific tool, another four solutions have been developed to deal with operational challenges during pandemics: risk-based access control (RIBAC), demand prediction and management (DPM) tool, solution for cyber-physical resilience (CPR), and remote infrastructure inspection (RII) solution. In this paper we will introduce all tools, before covering in more details CPR (Juan Fidalgo, 2023), consisting of four main modules (AI-powered log monitoring, security risk assessment tool, incident response management tool and threat intelligence sharing platform).

3. PROJECT MAIN CONCEPTS

While sudden adverse events may cause rapidly severe and immediate damage in critical infrastructure, events like the COVID-19 pandemic start slowly, so that the operational conditions that impact CI have several changes over time. The advantage of dealing with slow crisis in contrast to sudden disasters is that potentially there is time to set or finetune risk mitigation measures and resilience strategies. However, this operational “adaptivity” approach needs to be modelled in advance.

Traditional risk management approach is mostly pre-event (adverse event probabilities, scenarios), while crisis management is mostly dealing with actions during these adverse events. The concept of resilience cuts across the timeline, focusing on performance and critical service provision over time. Resilience unites time and space, it englobes, for example, design of

systems to absorb shocks in time, detection and mitigation to limit spatial propagation, or post-event recovery over both time and space.

SUNRISE project delivered a step-by-step process on how the different concepts, methodologies and tools from the project can be applied in a structured way to improve the resilience of critical infrastructures. Since risk and resilience are related concepts, the approach was also to reuse concepts and approaches from risk management. In a matter of fact, some critical infrastructure (CI) risk indicators and metrics can be re-purposed for CI resiliency. In (Mentges, 2023), for example, in depth definitions and glossary analysis are performed and authors also review boundaries of this term, i.e., what is not resilience. They highlight that risk management focuses on identifying and avoiding/reducing the impact of foreseeable and specific threats, while resilience management focuses on a holistic increase of the ability to deal with disruptions as they emerge, emphasizing the time dimension (e.g., recovery after the initial disruption).

Both risk and resilience assessments calculate impact and/or performance loss, but resilience also considers recovery function and therefore has an important temporal dimension. We can conceptualize temporal aspect of digital infrastructure resilience in five areas: Identify, Protect, Detect, Respond, and Recover, which while being iterative process, can roughly match time periods before, during and after incident occurs.

In the "classical" absorptive capacity approach, static risk assessment is done only "BEFORE" incident. However, in SUNRISE, at least when it comes to operational cyber resilience, the real time ingestion of relevant risk indicators is enabled, and it is used to trigger risk re-assessment at any moment also "DURING" adverse event, when operational conditions change rapidly. This is important since there are properties of infrastructure under assessment (e.g., complexity, dependencies) and external context (e.g., threats, hazards, or other risk indicators that are consequence of temporary situation such as pandemics) that need dynamic assessment (e.g., incident on a specific day might not have the same impact as on the other days). While continuous risk assessment is virtually impossible, we did apply frequent reassessment triggered each time a new set of risk indicators meets certain criteria or threshold.

Measures implemented to contain pandemic spread, such as non-pharmaceutical interventions (e.g. lockdown, geographic restrictions) sometimes destabilize normal maintenance and support of infrastructure or result in derived operational risks. Frequent changes of priority also had an impact, as well as the dynamics of collaboration with the public authorities or other operators of CIs. The functioning was unpredictable due to the interruptions in supply chain and increased use of remote working tools, which resulted in an unprecedent need for adaptivity.

On of the concepts introduced to deal with this need for adaptivity at operational level is so called "temporary conditions model", with variables and values that might not directly affect organizations or critical entities in the same way as they affect people or technology. For example, the remote work might have impact on technology (e.g. AI-based anomaly detection relies on the patterns of connectivity used for AI training), on procedures (e.g. incident response and obligatory reporting), or on human factors (e.g. awareness about the use of remote workstations for the personal use or other way round).

We also argue that for the fast-changing situations and contextualization of the available information in rapidly changing circumstances, approach based on Observe, Orient, Decide, Act (OODA) loop at operational level is more appropriate than Plan, Do, Check, Act (PDCA) approach, which is often used at strategic level for mid to long term planning. Dynamically changing operating condition variables and values, might refer to anything, from workforce absenteeism to threat probability, although "temporary conditions model" was applied only for cyber resilience tool in SUNRISE. Regarding the identification of vulnerable essential employes, for example, identification could be done with data available from Human Resources, but finding those that are indirectly vulnerable (e.g., they must take care of infants or the elderly) would be much more difficult. As a result of pandemics, major psychological pressure is detected among employees. This could be linked to the impact of phishing and other types of cyber-attacks in temporary conditions, widely discussed in (Kioskli, 2023).

For this reason, flexible model with different categories of attributes and variables was adopted for the "temporary condition model" and the adaptation of automated cyber-risk re-assessment in SUNRISE cyber resilience tool. These can refer to the ability of operators to perform their work, influenced by pandemic factors such as fear or general rules such as social distancing, but also availability of resources at operational level, including human (e.g. absenteeism) or external data availability. Other parameters are organization of business sector specific, such as dynamic changes in digital asset model (e.g. value at risk), working conditions, supply chain disruptions, security policies (functions that are not allowed to be conducted off premises) etc. In SUNRISE cyber physical resilience (CPR) tool context, we link disruption of critical service to cybersecurity incident, which might be consequence of a specific cyber threat, but also considers physical risk indicators such as workforce availability. Our aim is to bring cybersecurity approaches in relationship with overall resilience of CI. For this reason, more attention was given to risk models that affect the availability of critical cyber assets.

4. APPLICATION TO CYBER RESILIENCE

Cyber resilience of CI, following the general definition of CI resilience, is therefore focused on CI operator ability to prepare for, respond to, and recover from cyberattacks that might have consequences for the infrastructure or provision of critical services. In a similar way, cyber crisis management in CI is focused on the coordinated management of emergencies caused by cyber-attacks. The European Union Agency for Cybersecurity (ENISA) publishes, for example, detailed cyber crisis management exercises and handbooks, including national-level crisis coordination guidance.

In scenarios such as pandemics, both cyber resilience and cyber crisis management, must consider temporary operational conditions created or derived by the overall resilience strategy and crisis management activities. Nature and speed of response in cyber crisis management is also different, compared to physical infrastructure resilience. Technical countermeasures, such as attack containment, reconfiguration or patching vulnerabilities, is not depending so much on physical properties but there is a strong dependency on experts and human knowledge, which in case of pandemics might not be always available.

While some cyber-attacks often demand near real-time responses, not all cyber incidents are treated as cyber-attacks. An incident could be any event that poses a potential risk to an organization's systems, data, or processes. Unauthorized access detected in a system or a phishing attempt, where no damage occurs, are incidents but also indicators of possible ongoing cyber-attack. The amount of time available to react during incident management, without experiencing any impact depends on multiple factors, including the nature of the incident, its detection speed, the organization's preparedness, and the type of systems or data involved. Automated defenses, such as firewalls and intrusion prevention systems, act immediately, based on predefined rules, to block attacks like a DDoS or brute force attempts. For certain attacks, however, manual intervention combined with automated tools is needed. So called "triage process" is often the initial step in incident handling and response and it involves evaluating, prioritizing, and categorizing security alerts or incidents to determine their relevance, severity, and required actions. The goal is to focus resources on genuine threats while minimizing false positives.

If an incident is detected early and contained before escalation (e.g., identifying and isolating a phishing attack target), reaction time window is longer. We might even have days to react for slower-developing threats (e.g., advanced persistent threats slowly exfiltrating data). In other words, not all attacks are same, but while the duration of specific reaction window varies, organizations with proactive measures and predefined response or course of mitigation actions are generally considered as more cyber resilient than others.

This is why semi-automated risk assessment is included in SUNRISE CPR solution as a basis to enhance the efficiency and accuracy of the triage process. Furthermore, it can also improve prioritization and ensure timely responses to threats. Automated systems can assign a risk score to alerts or incidents based on risk model, severity of the threat, contextual data (business impact such as asset criticality or operational conditions such as availability of work force), but also based on external data such as Indicators of Compromise (IoCs) received from threat intelligence feeds. Enriched data can provide analysts with actionable insights, speeding up triage, so the more complete IoCs are, the better it is for the cyber resilience.

One could argue that cyber-attacks, like pandemic events, show dual nature of both slow and rapid-onset adverse event, and that a window of time to react depends on detection of early symptoms in a pandemic and early warning signs of a cyber-attack, such as network or access anomalies. Observation of "early warning" signs or events, and their use as risk indicators, was therefore the second important consideration for design of SUNRISE CPR solution.

This temporary model is overwriting default operating values and is addressing awareness of the dynamic cyber threat landscape related to and/or implied by pandemics, as well as improved estimations of probability and impact in risk assessments for cyber threats under temporary conditions.

We have conceptualized temporal aspect of cyber resilience with time periods before, during and after incident occurs (figure 1). A typical way to assess CI resilience including this temporal dimension is to use the performance loss and recovery function. In this context we consider cyber threats as a "threat multiplier" during pandemics, like e.g. disruption of supply chain or other risks to CIs. A threat multiplier is a factor that amplifies the severity, scope, or

impact of an existing risk or challenge. It does not create the initial threat but can make consequences worse. During a pandemic, for example, cyberattacks targeting healthcare systems (e.g., ransomware attacks on hospitals) can disrupt patient care, vaccine distribution or trust in vaccination, recovery, and test certificates. Cyberattacks can also trigger cascading failures across sectors, for example attack on an energy grid or water management can paralyze other sectors. In SUNRISE, we also consider "threat multiplication" in the other way round: pandemic as a threat multiplier for cyber resilience. Social engineering attacks (e.g., phishing) exploit fear or uncertainty, while many other attacks are more likely to succeed when organizations are already under-resourced. Cybercriminals often strike during or after other crises when defenses are lower, and absenteeism is high. They also exploit the urgency, fear, and increased reliance on new or untested technology to carry out malicious activities.

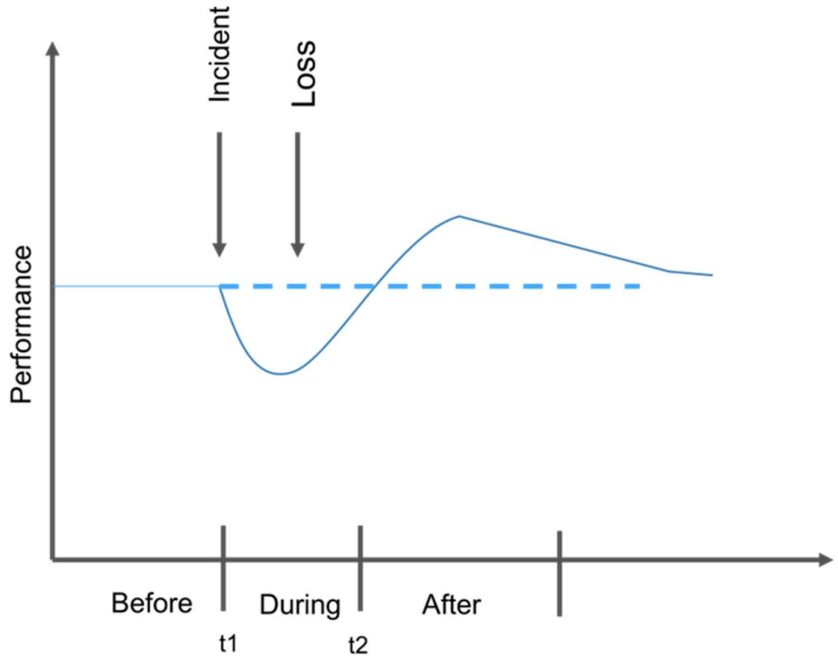

Figure 1: Typical resilience time-performance function

One of the implemented novelties in SUNRISE CPR is cyber risk assessment re-triggering "DURING" an incident (in cyber crisis management phase), enabled by the real time ingestion of relevant events that serve as the risk indicators. One example are events from AI-powered log anomaly detector, adapted to reconsider what is "anomaly" under the temporary pandemic conditions (e.g. more remote connections at unusual times). Other examples that re-trigger cyber risk assessment during an incident are changes in probability of attack escalation (e.g. due to the new information from threat intelligence sharing platform) or changes in pandemic-specific priorities (e.g. attack on healthcare application for COVID vaccination has a high impact). Thanks to collaboration and information sharing with the other CI opeators, we can also address cognitive bias better, and work better with uncertainties, partial information, diversity or degree of randomness or information disorder. This is why integration of internal real-time cybersecurity event data with external threat intelligence is another essential

ingredient for cyber crisis management, timely risk assessment and response. It enables dynamic probability assessment thanks to the collaboration with other CI operators and governmental authorities, while SUNRISE specific threat scoring module calculates timeliness, relevance, trustworthiness, and other parameters used to readjust initial risk values. These dynamic risk assessments directly impact "absorption" of an incident, thanks to the early identification of an attack, and reduction of mean time to react (MTTR).
Finally, managing data about absenteeism in cybersecurity operational teams is another novelty, used to reflect actual situation in operational context. Increasing number of the available security experts during specific time window or setting priority according to their availability is an example of risk mitigation adaptivity. Mapping of external operational indicators of compromise (IoC) to cyber-attack techniques, tactics, and procedures (TTP) also increases adaptivity as it focuses on contextualization of the available information, while making sense of newly arrived external data and changes during temporary conditions (e.g. trust in external threat intelligence source). It is a particularly suitable approach for volatile, uncertain, complex, and often ambiguous inflow of risk related data, such as the case of pandemics.

5. CONCLUSIONS

The COVID-19 pandemic was an example of a temporary situation when critical infrastructure (CI) had to operate with continuously changing conditions. This was reflected in changes of cyber-risk assessment and cyber crisis management, and in consequence, also changes of overall resilience assessment for CI. The move to remote working, absenteeism or relaxing cybersecurity policies are some examples considered in design of adaptive SUNRISE cyber-physical resilience.
In the realm of cyber resilience and crisis management, there are other specificities compared to the general concept of resilience in CI. Adverse events are cyber-attacks, man-made and voluntary, and therefore study of the source of cyber threats, including studying threat actors, their motivations, capabilities or TTPs (Tactics, Techniques, and Procedures), is very important. Technical countermeasures, such as reconfiguration, patching vulnerabilities, or rerouting traffic, is not depending so much on the availability of physical resources like in the case of general resilience, but there is a much stronger dependency on cyber experts and human knowledge, which in case of pandemics might not be always available.
In SUNRISE project, we designed and developed highly adaptive cyber-physical resilience solution based on cyber risk-driven approach that benefits from intelligence sharing, application of temporary condition parameters and threat-driven re-assessments, aligned with the organization's broader priorities or workforce availability.
By combining sensing ("observation") of external environment (incidents from security information and event management (SIEM), threats from intelligence sharing platforms, vulnerability from scanners, abnormal behavior events, etc.), with a cognitive process of "orientation" (including threat score calculation or mapping to tactics, techniques and procedures), we developed solution that was validated in various pilots with CI users in Slovenia and Italy.
The most important conclusion was about how sharing and enhancing threat intelligence can have several impacts on CI resilience and crisis management, including awareness about dynamic changes and temporary conditions, improved detection capabilities (e.g. decreased time to develop or fine-tune security controls, such as new rules for intrusion detection systems or multi-factor authentication), as well as improved decision-making to allocate scarce resources more effectively, by prioritizing security controls and countermeasures.

There is still work to do in the SUNRISE project and beyond, including extension to risk indicators that cover behavioral aspects. In addition, we need currently to run risk re-assessment every time there is a significant change of risk indicators. This might lead to "assessment fatigue" or even congestion in decision making. Finetuning might be needed to reach balances and work on trade-offs between dealing with dynamicity and tool practicality.

6. REFERENCES

Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

CER Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Juan Fidalgo P., Pasic A., Del Álamo J.M., Tourís R. and Álvarez A. (2023), "TERME: a cyber-physical resilience toolset for risk assessment," JNIC Cybersecurity Conference (JNIC), Vigo, Spain, pp. 1-6, doi: 10.23919/JNIC58574.2023.10205687.

Mentges, Andrea & Halekotte, Lukas & Schneider, Moritz & Demmer, Tobias & Lichte, Daniel. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. 10.48550/arXiv.2302.04524.

Kioskli, K., Mouratidis, H., Polemi, N. (2023). Bringing humans at the core of cybersecurity: Challenges and future research directions. In: Abbas Moallem (eds) Human Factors in Cybersecurity. AHFE (2023) International Conference. AHFE Open Access, vol 91. AHFE International, USA. http://doi.org/10.54941/ahfe1003722