OPPORTUNITIES FOR IMPROVING CYBER RISK MANAGEMENT IN CRITICAL INFRASTRUCTURES

Aurelian BUZDUGAN
aurelian.buzdugan@yahoo.com

CZU: 004.056.53:005

Introduction. Cyber risk management has become one of the core priorities in ensuring the safe and secure functionality of critical infrastructures (CIs). These facilities are often at the core of our economy, transport, communication or national security. The international character of cyber security, as well as the safety events that a cyber attack could lead to, are mandating new ways to identify and control these risks. The paradigm of physical security in terms of fences, guards and locks includes now the cyber security controls as well. The risks arising from the use of digital technologies range from computers used in the monitoring and control rooms, up to sensors and IoT devices, thus specialized knowledge is required. Therefore, risk management process needs to adapt to the new threat landscape and ensure that emergent risks are tackled adequately.

In this paper we will review the progress of identifying the core areas in cyber risk management for CIs. We will present the elements that we believe are necessary to take into account upon using decision support systems (DSS) for managing risks in this domain. We will also propose future research directions in the adaptation of DSS for the cyber risk management.

Current research areas. The current threat landscape of a CI is characterized by an increasing number of cyber attacks. Moreover, the integration of IT technologies in physical systems create new venues of attacks. If physical security controls have been adapted over time to ensure the safety of the facility, and the systems in charge of control and monitoring were mostly analogue, the emergence of information technologies in the last decade has created both opportunities as well as created new risks. Computer technologies, in any form and scope used, are a potential target in the cyber space. The attacks can be launched from virtually anywhere in the world, without a need to be physically present in a specific facility. History has also proven that concepts such as “air gap”, where a system has no direct connection to Internet, are no longer effective as these create a false sense of security. For example, the StuxNet malware, has demonstrated that remote exploitation of a system from a CI is possible, and could moreover lead to safety events.

The analysis that we have performed on risk management in critical infrastructure has included papers from reputable sources, such as research journals or international organizations [1,2]. We have learnt about the areas of risk management that are a focus of current research, and mainly processes concerning the identification, evaluation and mitigation of risks [3]. We found that the grouping of cyber risk identification, prioritization and mitigation has not broadly been explored yet [4]. Taking into account the current threat landscape as well as that digitization of the society, we stress upon the importance of a comprehensive risk management process that would cover scenarios of cyber-attacks as well. We believe that one way to tackle emergent risks is by using computing systems.

Another conclusion from the review performed is the opportunity of using DSS in enhancing the risk management process. This would support decision makers or operators in managing cyber risks within CIs. We believe the explicit integration of cyber risk management in the overall risk management method is required. Taking into account that most risk methodologies are focused on generic type of risks and do not cover explicitly the cyber risks, there gaps could be fulfilled by developing decision support system, as modules, that could be integrated in other methodologies or frameworks [4]. Among the elements that we proposed to be addressed by a DSS are the context, the target users, digital components of the CI and their interconnection, cyber-attack methodologies and tools as well as resilience [4]. The DSS would support, inter-alia, the live collaboration between decision makers and operators [5], analysis of large amount of data such as vulnerabilities and potential mitigations, as well as simulations on the impact of a change in the system given the interconnections between the CIs. This solution would improve the accuracy and decision-making capability in managing cyber risks

Conclusions and future recommendations. Cyber risk management is a complex process that requires the analysis of a large amount of various data. This could include information such as the use and function of an IT system, the functions this system performs, potential impact on operational technologies as well as the interdependency between cyber-physical systems. Even if this domain is relatively new and requires specialized knowledge, there are opportunities to facilitate this process by using decision support systems. These are in our opinion an adequate solution to improve the decision making capabilities in critical infrastructures. We have identified the elements required to be assessed during design and development, in order to ensure the DSS would be efficient and adapted to the needs of CI domain. This creates new potential areas of future research in the development of the DSS, such as the integration of artificial intelligence elements as well as the methods of integrating DSS into risk management methodologies.

Referfences:

1. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen (2012). *Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art.* Available at*:* https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf
2. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen (2015). *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach.* Available at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf
3. BUZDUGAN, A., CĂPĂŢÂNĂ, Gh. Factors for a decision support system in critical infrastructure cyber risk management. In: *Romanian Cyber Security Journal.* 2020.
4. ANI, D.A., et. al. (2019). *A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape.* Available at: https://arxiv.org/ftp/arxiv/papers/1904/1904.01551.pdf
5. FILIP, F.G. (2020). DSS – A Class of Evolving Information Systems. In: DZEMYDA, G., BERNATAVIČIENĖ, J., KACPRZYK, J. (eds) Data Science: New Issues, Challenges and Applications. Studies in Computational Intelligence. *v*ol 869. Springer, Cham. doi:10.1007%2F978-3-030-39250-5_14