Factors for a Decision Support System in Critical Infrastructure Cyber Risk Management

Aurelian BUZDUGAN, Gheorghe CĂPĂȚÂNĂ
Universitatea de Stat din Moldova
aurelian.buzdugan@yahoo.com, gh_capatana@yahoo.com

Abstract: Cyber risk management is heavily reliant on the processing of a large volume of risk data and a complex process of analyzing, prioritizing and decision-making. The interconnection, interdependence and digitalization of critical infrastructure considerably increase the amount of data that needs to be assessed when managing risks. Specialized knowledge in cyber security is required in order to efficiently assess the risks posed by an IT system on an entity. The amount of data required to be processed in the decision-making process goes beyond the human limits and computer systems should be used to support this process. In this paper we evaluate how cyber security fits into risk management approaches for critical infrastructure. We explore particular factors of cyber risk management in this area, as well as the challenges these create for operators and decision makers. One of the key areas we evaluate is whether the existing risk management process adequately tackles the cyber risks. We identify the areas where further developments are required as well as propose criteria for a decision support system that we believe will improve the cyber risk management in critical infrastructure protection.
Keywords: cyber security, risk management, critical infrastructure, decision support systems

INTRODUCTION

The paper begins with an overview of critical infrastructure (CI) role in the current societal context and the challenges in managing cyber risks in this domain. We will look at the elements of the risk management methodologies that are currently being applied to CI. In addition, we want to explore the needs and requirements in terms of managing cyber risks within CIs, by relating to current knowledge and experience from the IT domain.

We will estimate the extent to which cyber security is included in the risk management for CIs, as well as identify good practices and approaches. To ensure the quality of our analysis we related to the latest developments and results in this area by selecting recent relevant research. As the scope of such an analysis is broad, it has been challenging to select the papers and research to be reviewed. Priority has been given to analysis papers related to risk management in critical infrastructure protection (CIP), in order to understand the views and challenges of decision making. Precedence was given to trustworthy sources, such as research journals, or reports from national or international organizations. Based on the analysis and observations we will extract key elements that challenge the risk management for CIP. Taking into account the increased

interest and use of decision support systems and their potential to address specific application domains *[Filip, 2014]*, we believe this would be a feasible solution for managing complex tasks. Therefore, we will also propose elements to be considered for a decision support system in the area of cyber risk management in CIP.

CRITICAL INFRASTRUCTURE AND DIGITAL SOCIETIES

The CIs are at the functional foundation of our society, economy, national security and other domains. They are also the focus of one of the major natural or man-made disaster risks that the EU might face *[European Commission, 2017]*. The critical infrastructures are now part of the cyberspace, and, given the interdependence between CIs, it has led to the inclusion of CIP among the urgent issues for national as well as international security *[World Economic Forum, 2020]*.

Nowadays, the more computerized a society is, the more vulnerable it could be. The interconnection and interdependence between these systems is inevitable at this point. This is shown in ***Figure 1***, together with the role of computer components in the context of a CI. We believe the figure is a realistic representation of the complexity of CIP process, where IT systems have a central role in monitoring or control activities, but also create additional attack surfaces.

A small disruption in any of the infrastructures could cause a domino effect, for example the disruption of the energy grid could lead to disruption in other sectors, such as transport or telecommunications *[Siemens, 2019]*. We noted a current emphasis on the energy sector, as this is often the driving system. For example, the nuclear sector has gone through a massive digitization process which requires nuclear and radiological operators as well regulatory bodies to ensure that digital assets are adequately protected. However, taking into account the development pace the CIs are going through, we believe risk management requires a holistic approach for the entire domain. The forecasting of cyber integration consequences in CIs is more challenging due to emerging technologies, which increase the cyber risk surface of contact.

Cyber threats specific to the CI are an evolving topic due to the dynamic and global character. In recent global studies, cyber-attacks on critical infrastructures were rated the 5th top

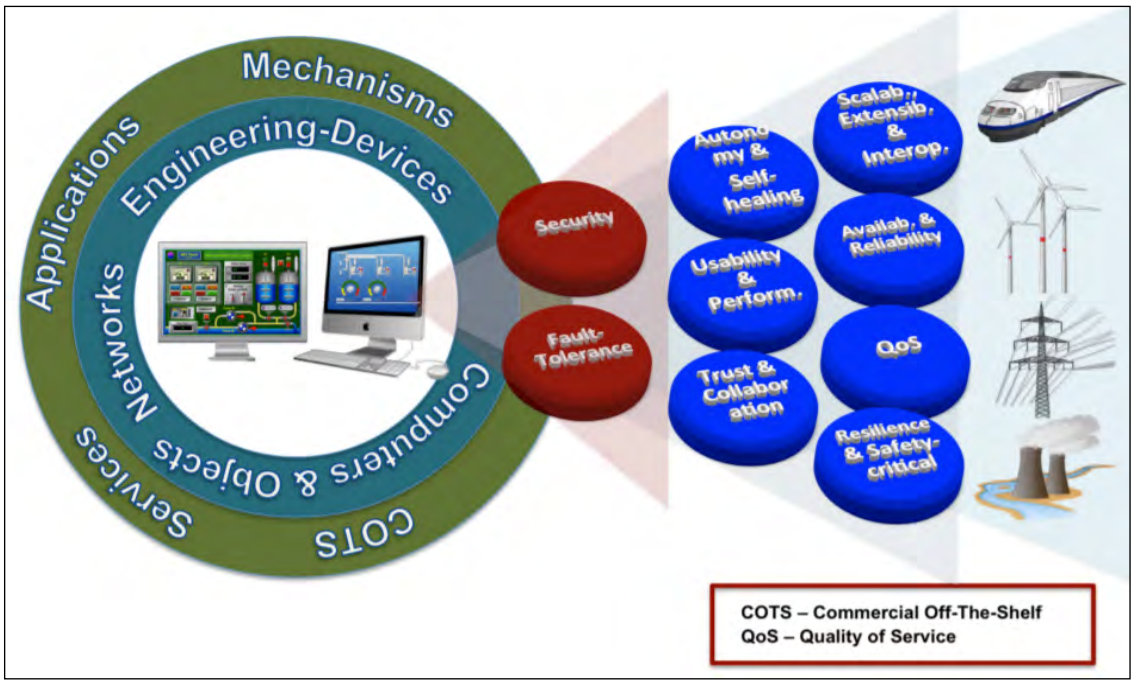

Fig. 1: *Security requirements to protect critical infrastructures (Alcaraz & Zeadally, 2015)*

risk for the year 2020, being able to affect entire cities or even countries *[World Economic Forum, 2020]*. Compared to traditional IT environments where mitigation measures are proportional to the impact and likelihood of the potential risks and security incidents, in CI the context becomes more complex to define. In addition, the control of a risk is much more demanding as cyber-attacks could lead even to a safety event. This trend is observed for domains that are critical to society, such as healthcare where cyber-attacks are on the rise in the last decade *[Healthcare Information and Management Systems Society, 2019; Deloitte, 2013]*.

The integration of IT, coupled with the specific requirements of CIs, create new challenges for both decision makers and operators. The risk assessment for CIs has a certain focus that is dictated by these environments, such as operation and availability. The emerging technologies challenge the existing approaches, as there appear new vulnerabilities and windows for malicious actors to disrupt critical systems. Therefore, the processes of identification, prioritization and mitigation of risks require evaluation through the prism of new technologies and challenges.

MANAGING CYBER RISKS IN CRITICAL INFRASTRUCTURES

The main scope of risk management is to prevent losses, damages or loss of functionality in a system, in our case a CI. It is obvious that a risk cannot be completely eliminated. Instead, after the risk identification, analysis and the implementation of certain mitigation measures, it could be reduced to an acceptable level. As cyberspace permanently generates new risks, a regular and continuous assessment of the associated risks is required to ensure the effective protection of data, services and CI functionality, taking into account the changes that occur.

In the process of managing cyber risks in a CI, we need to understand that computerized systems are at the core of control, monitoring and detection systems. It is vital to establish the context and identify the parameters that are required to assess these risks. By comparison to risk management in traditional IT systems, the CI safety and resilience elements are unique and create new challenges. To ensure that the CI risk management is appropriate, it is essential to evaluate during the assessment phase all of the elements and define the context (activity of the CI, relation to other CIs), the risks in terms of potential problems, the security concepts being followed as well as the limitations of the system *[National Institute of Standards and Technology, 2016]*.

We will continue our analysis with the risk management elements in the CI domain that are central in the view of emerging IT technologies. ***Figure 2*** presents the proposed criteria to be considered when developing a decision support system for risk management in critical infrastructures.

These elements will define new requirements and could improve the methodology of defining risks and identifying appropriate mitigation measures. We will describe the identified elements below and evaluate their implications for the overall risk management process. These elements will be considered for a decision support system concept in the risk management process.

Target audience

Approaches in cyber risk management tend to be different in scope and content, as these capture data to be considered by a specific audience. For example, certain approaches are targeted to senior management and decision making, whereas other to the operators of the CI. As such, cyber security risk management should not only be treated as a technical function, performed by IT or operational technologies (OT) experts, but as a complex process oriented towards the integral management of the CI object or system. The description of cyber security risks needs to be clear for both decision makers, as the ones who manage risks, as well as operators, who are the ones implementing mitigation measures for these risks.

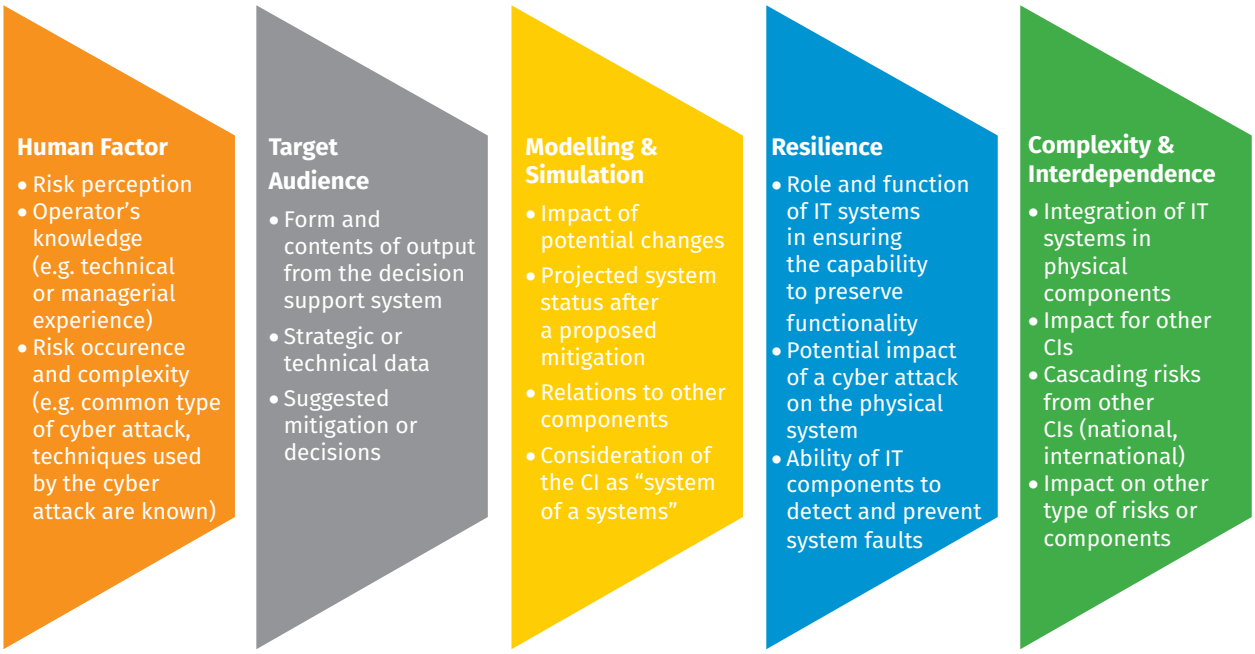

Fig. 2: *Elements to be considered for a decision support system in risk management*

Resilience

The cyber risk management applied in the field of OT and CIs brings a new dimension, which is resilience *[European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, 2012]*. Resilience shows the capacity of a system to absorb and buffer any anomalies or unexpected changes, as well as recover and continue operations *[European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, 2015]*. This is a new element not often met in traditional IT risk management approaches. Whereas there are tendencies to ensure the resilience of IT systems by having this as a core requirement, the common aspects currently considered are represented in the CIA triangle (Confidentiality, Integrity, Availability) which indirectly cover resilience as well. This approach can also be applied to IT and OT, however due to the specifics of CIs the explicit requirement for resilience is mandatory in order to ensure at all times the availability and operation of the system. In the cyber-physical systems, resilience is linked to fault tolerance and suggests that physical systems continue to operate under various conditions, even if certain parameters could take on anomalous values. From the CI perspective, it can be indirectly deduced that computer systems in charge of a function should detect and tolerate faults, in order to avoid any cyber related incidents that could lead to the malfunction of the physical system.

We consider the element of assessing resilience within risk management to be a challenge, as any component of a system needs to be part of a comprehensive modelling and simulation process in order to understand the impacts of changes. Assessing this element in the context of emerging IT technologies in CIs can constitute a even more complex task.

Modelling and simulation

Modelling and simulation (M&S) are important tools to evaluate potential changes in a system over time, as well as create the ability to forecast the dynamics of a system. M&S can be used to analyze the interdependence and interconnection between CIs, as well as the impact of any change in any component across the entire system *[Ani et al., 2019]*. The functionalities, technologies and operations of a CI are used to model the effects of implementing security controls and estimate the results after a change. This is very useful in

the context of risk mitigation and in the overall process of risk management in CIs. However, as there are different approaches in the protection of CI systems, it is still a challenge to choose the most effective one due to the complexity of these systems.

In addition, M&S for CIs already adopted the idea of system of systems. It is hard to think of a CI that, today, exists in isolation. For example, most, if not all, CIs would be dependent on energy supply. This complicates the risk management process due to the quantity and hierarchy of systems to be considered. Furthermore, enriching data with the connections between CIs, whose elements may be spread cross-border as well, increases significantly the volume of risk data. Similar to the IT domain, the system of systems concept complicates the assessment and requires modelling techniques.

Modelling can be used in the risk management processes for emerging technologies such as IoT, and help evaluate the cyber risks *[Alcaraz & Zeadally, 2015]*. This would support the understanding of changes in a CI by utilizing various perspectives. Current research shows that the most common modelling techniques used in CIP are empirically based *[Ani et al., 2019, Ouyang, 2014]*, whereas protection-based cyber-attack assessments are easier to adopt *[Rabe et al., 2018]*. These findings help contour a new approach in ensuring cyber security and would refine the output from a decision support system in evaluating risks and mitigations.

Complexity and interdependence

Complexity and interdependence are other particularities of risk management in CI. The cyber dimension is integrated into the physical system, which ultimately creates new demand for knowledge required to manage risks. CIs could often be referred to as cyber-physical systems, which derive the requirement to have both types of knowledge and experience for managing risks *[König et al., 2019]*. The cyber-physical link is widely reflected in research as the increase of attack surface by having embedded computers in physical systems responsible for operations *[Choraś et al., 2016]*. This leads to an increase of potential vulnerabilities as well as attack vectors. Consequently, cyber security should already be included in the overall risk assessment plans for any CIs and treated as an intrinsic part.

Human factor

The human factor plays a vital role in risk management for any domain. One implication of the human factor is that accuracy decreases as the complexity increases, which is associated with CIs as well. Risk assessment methodologies often take into account one risk linked to a specific component or its functionality. When it comes to a cyber attack that could affect a component, often interconnected, it requires modelling and simulations in order to understand the precise impact on all other components and systems. As a CI is considered a system of systems, and IT components are integrated in most of them, it creates complexity for the decision makers. This also applies to the identification and selection of appropriate countermeasures.

Another important human factor in cyber risk management is the perception. Recent studies illustrate that experts were more aware of vulnerabilities for which attacks were reported more frequently *[Ellerby et al., 2019]*. This is potentially due to familiarity and specific knowledge of this system based on the incident reports. In addition, the perception is that it is harder to conduct an attack on systems that are more technologically mature, or by not knowing the maturity level *[Ellerby et al., 2019].* This shows the need for specialized knowledge in different areas, to increase the effectiveness and quality of the risk identification and evaluation process.

Risk management has not only merged into a more complex process, but also requires real time collaboration between more parties on complex decisions *[Filip, 2020]*. The human factor also links to challenges in developing the security culture for operators and management, and utterly on risk management in CIs. When it comes to presenting the risks and informing other stakeholders, the human factor needs to be considered. These recommendations should

be reflected in the design of a decision support system for risk management.

We believe the support for the decision making is mandatory in order to understand the full impact of cyber risks upon a CI system, as well as identify the appropriate controls to reduce these risks. We believe modeling or decision support systems are the right approach in analyzing different data inputs and providing human understandable outputs.

CONCLUSIONS AND FUTURE RESEARCH

We have ascertained that general risk management processes such as identification, assessment and control implementation are of current interest in research *[Ani et al., 2019]*. The cyber security risks in CI are an emergent topic due to recent attacks as well as the critical role of the IT components in physical systems. We also remarked that the combination of cyber risk identification, prioritization and mitigation is an insufficiently explored area. Taking into account the number of approaches in CIs, we believe risk management should be holistic and have scenarios covering the cyber risks as well. This highlights potential future research in defining a decision support system to identify, prioritize and potentially propose controls that would effectively manage cyber risks in CI.

Based on the analysis, we note that the risk management process is becoming more complex, and often crafted and adapted to the needs of each type of CI. Our outcome is that cyber risks are included within the general risk management process, but these risks would be better identified and managed when having specialized knowledge. Very few methodologies were evaluating exclusively the impact that IT and cyber security have on CIP, as a separate module or process. We believe that for an effective cyber risk management in CIs, it is necessary to improve the accuracy and decision-making capability.

We recommend to facilitate this process by using decision support systems. The elements that should be considered by this system are: the knowledge about the CI system and its digital components, cyber-attack methodologies and tools, resilience, interconnection, dependence and human readable outputs. As these elements could imply large amounts of specialized data, the decision support system would help senior management in identifying risks and selecting the best package of mitigation measures. This would be, in our opinion, a system that would promote the secure and safe use of emerging technologies in the context of CIs, contribute to a better security stance and increase its overall security outcomes.

We believe that the present analysis and recommendations will contribute to the improvement of methodologies used for cyber risk management in CIs, by assessing current and future development of emerging technologies. We have also identified the factors that will contribute to the development of a decision support system to aid this process. Further study is required in order to develop and improve this technique for managing cyber risks in the critical infrastructures.

ACKNOWLEDGEMENTS

The presentation of this article was possible due to the doctoral project “Decision support system for identifying and reducing cyber risks in critical infrastructures”.

REFERENCE LIST

Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection. 8. 53-66. Available at: https://www.nics.uma.es/sites/default/files/papers/alcaraz%3A2015%3ACRI.pdf [Accessed 20 Mar. 2020]

Ani, D.A., Jeremy, D.M., Watson, J.R., Nurse, J., Cook, A., Maple, C. (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 [Accessed 20 Mar. 2020

Choraś M., Kozik R., Flizikowski A., Hołubowicz W., Renk R. (2016). Cyber Threats Impacting Critical Infrastructures. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, vol 90. Springer, Cham. doi:10.1007/978-3-319-51043-9_7

Deloitte (2013). Networked medical device cybersecurity and patient safety: Perspectives of healthcare information cybersecurity executives. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf [Accessed 20 Mar. 2020]

Ellerby, Z., McCulloch J., Wilson M., Wagner C. (2019). Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security. Available at: https://www.researchgate.net/publication/336230531_Exploring_how_Component_Factors_and_their_Uncertainty_Affect_Judgements_of_Risk_in_Cyber-Security [Accessed 20 Mar. 2020]

European Commission (2017). Overview of Natural and Man-made Disaster Risks the European Union may face. Available at: https://ec.europa.eu/echo/sites/echo-site/files/swd_2017_176_overview_of_risks_2.pdf [Accessed 20 Mar. 2020]

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 [Accessed 20 Mar. 2020]

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 [Accessed 20 Mar. 2020]

Filip, F.G., Suduc, A.-M., Bîzoi, M. (2014). DSS in numbers. Technological and Economic Development of Economy, 20(1), 154-164. doi:10.3846/20294913.2014.890139

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, vol 869. Springer, Cham. doi:10.1007%2F978-3-030-39250-5_14

Healthcare Information and Management Systems Society (2019). HIMSS Cybersecurity Survey. Available at: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf [Accessed 20 Mar. 2020]

König, S., Rass, S., Schauer, S. (2019). Cyber-attack impact estimation for a port. In: Jahn, Carlos Kersten, Wolfgang Ringle, Christian M. (Ed.): Digital Transformation in Maritime and City Logistics: Smart Solutions for Logistics. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 28, ISBN 978-3-7502-4949-3, pp. 164-183. Available at: https://www.econstor.eu/bitstream/10419/209392/1/hicl-2019-28-164.pdf [Accessed 20 Mar. 2020]

National Institute of Standards and Technology (2016). NIST Special Publication 800-160, Systems Security Engineering. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf [Accessed 20 Mar. 2020]

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety, Elsevier, vol. 121(C), pages 43-60. doi: 10.1016/j.ress.2013.06.040

Rabe, M., Angel A.J, Navonil M, Anders S, Shefali J., Birger J. (2018). Cyber risk of coordinated attacks in critical infrastructures. Available at: https://pdfs.semanticscholar.org/0d49/8506ff4d764f87e9770827227db62acb1a14.pdf [Accessed 20 Mar. 2020]

Siemens (2019). Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat? Available at: https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf [Accessed 20 Mar. 2020]

World Economic Forum (2020). The Global Risks Report 2020. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf [Accessed 20 Mar. 2020]