INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

Publisher
http://jssidoi.org/esc/home

INDUSTRIAL CONTROL SYSTEMS (ICS) CYBER PREDICTION MODEL*

Joana Katina [1], Tomas Plėta [2], Romualdas Petkevičius [3], Lina Lelešienė [4]

[1,] Vilnius University, Institute of Computer Science, Department of Computational and Data Modeling, Didlaukio st. 47, LT-08303 Vilnius, Lithuania
[2]Vilnius Gediminas Technical University, Saulėtekio Ave. 11, LT-10223 Vilnius
[3,4]Mykolas Romeris University, Ateities St. 20, LT-08303 Vilnius, Lithuania

E-mails: [1]Joana.Katina@mif.vu.lt; [2]Tomas.Pleta@gmail.com; [3]Romualdasp@gmail.com; [4]Lelesiene.Lina@gmail.com

Received 10 January 2023; accepted 12 March 2023; published 30 March 2023

Abstract. Acceleration of scientific and technical progress, speeding up of technological changes, IT process globalisation and integration of OT processes invoked new challenges in preparing cyber strategies. Issues with adapting strategy for a particular specificity, region and specific cyber-attacks are not applicable. Therefore, a natural need arises to adjust the process for future cyber-attacks. It should be noted that the vast majority of organisations still need to possess a strategy that has been developed in correlation with future cyber-attacks. A part of organisations, irrespective of the lack of methodology and necessary infrastructure at the initial stage, commenced applying strategic management methods as a more dynamic environment demanded adequate changes in the cyber security within the organisation itself. The organisation started to plan such changes because, at the initial stage of the strategic management theory development, the strategy was understood as a plan drawn up to achieve the set objectives, regardless of the future need. Implementing such strategic procedures is grounded on something other than scientific calculations and is often associated with excessive use of funds. Therefore, the main goal of this article is to determine how much the r-Interdiction Median Problem with Fortification (RIMF**)** module can be used as a model for deciding methods for protecting critical infrastructure systems.

Keywords: cyber security; fortification; critical infrastructure; r-Interdiction Median Problem with Fortification

Reference to this paper should be made as follows: Katina, J., Plėta, T., Petkevičius, R., Lelešienė, L. 2023. Industrial Control Systems (ICS) cyber prediction modeL. *Insights into Regional Development*, 5(1), 86-96. http://doi.org/10.9770/IRD.2023.5.1(6)

JEL Classification: O38

Additional disciplines: Information technologies

1. Introduction

Critical energy infrastructure often includes smart grids, which are used either for remote control or industrial automation contingent on electronic computers. These systems use two-way communication with a focus on the computational processing of information. It is a technology that has been widely used for several years. Well-established in energy production and management plants, a smart grid invokes the available resources by utilising

* *The research was partly financed by project "The Impact of Technological Progress of Industry 4.0 on the Development and Value of Industrial Production Sector"ITPI4, No 09.3.3-LMT-K-712-19-0037 (2014-2020 Measure No. 9 of priority 9 "Education of society and increasing the potential of human resources" of the action program of investments of EU funds)*

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

a variety of operating tools and energy measures such as power control and energy production. A smart grid integrates the capabilities of information technology and networks with those of smart management. The exchange of information takes place in real-time with the help of various devices that need to be operated within a critical infrastructure by applying new algorithms. Smart grids can detect faults and problems in a system, such as energy automation, production and management systems. The available resources of the system in critical infrastructure are utilised due to their ability to analyse in real time, thus, meeting the requirements (Tvaronavičienė, Plėta, Beretas, & Lelešienė, 2022). It is easily scalable and can be connected to other energy plants supporting common technologies (Bitirgen & Filik, 2023). Smart grids offer two-way communication; these are crucially important security issues, or else the reverse flow of electricity can cause security problems and reliability increases simultaneously in the critical industrial infrastructure.

A smart grid in critical infrastructure must be adequately protected against external factors. Despite its convenience and reliability, it poses security challenges (Somogyi & Nagy, 2022). Smart grids feature a significant pathogen; precisely, they integrate information into the network that will entail the ci issues as this network uses industrial equipment communications and all digital devices, making it vulnerable to cyber-attacks and malware infection. A targeted attack on a smart grid is aimed at intercepting sensitive information, taking over personal data and, finally, taking control of automated industrial operations. As mentioned above, smart grids are always a part of critical infrastructure and are adequately protected for their ability to interact with other intelligent devices such as IIoT. Inadequate configuration on smart devices that interact with the smart grid can be a gateway for intruders to the smart grid. Finally, innovative/supervisory operational teams involved in critical industrial infrastructure are an essential advantage as they can significantly improve communication within the infrastructure and avoid possible decisions that eventually lead to vulnerable systems in the future.

Smart grids offer significant benefits to later rendered critical infrastructure and industrial infrastructure in general; therefore, the citizens then receive these benefits as an organised critical infrastructure can provide high-quality benefits mainly to citizens with lower costs, including the security of energy production. In conclusion, the success of smart grids lies in the modern management techniques, their use, and the operation of all the teams involved in a critical industrial infrastructure, which provides an enhanced ability to solve many issues that may occur.

Some countries are facing problems related to the application of new technologies, including smart grids, due to the complexity of the state's legal system implementing the necessary cultivation permits and regulations, resulting in the inefficiency of critical infrastructure and services rendered. The energy plants that are also classified as critical infrastructure were created years ago; some of their functions at the time of their initial operation had low priorities, or these functions were not intended for upgrades that may be expected in the future. Only efficiency production was a priority, neglecting cyber-security. These systems were designed for another era when the needs for energy production were less demanding. Later, the necessary improvements had to be gradually made to meet the increasing demand for energy production. Cyber-security concerns in making these upgrades were only sometimes the priority.

Studies on cyber-security strategies and improvement of existing systems are based on a theory called "Game theory", in which blockchain models are integrated into multiple levels of programs also known as "Leader - follower". This hierarchical optimisation process presents the problem, where both the leader and the follower want to optimise their position at the same time, while the follower's solution is the reaction to the leader's solution. Optimal protection in critical infrastructure must be applied in such a way as to significantly reduce the rate of information loss and process failure (Parvasi et al. 2020). At this point, it is worth mentioning that, nowadays-critical infrastructure is significantly less vulnerable than in the past (Almaleh, & Tipper, 2022).

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

The goal of the research. Cyber strategy is a long-term planning tool, and it needs to have future insight to develop. Developing cyber strategies is mandatory for planning technical capabilities to protect organisations from cyber threats. It is a necessary forecast for future cyber-attacks, which should be integrated into cyber security strategy.

Methodology. The article analyses scientific research on the description and practical application of the r-Interdiction Median Problem with Fortification (RIMF) method. The paper describes the theory of the method's origin and analyses its use. One example of the practical application of the method was selected to achieve this goal, which was carefully analysed and described. At the end of the article, a conclusion was drawn on how realistic it is to use this method for integration into a cybersecurity strategy.

RIMF model intended to identify cyber threat recognition practices for protecting critical infrastructure can be applied. The RIMF model is an extension of the RIM model, as a tracking model for identifying protection practices of essential infrastructure systems. For the implementation, the RIMF model is divided into **two categories**: the external category, which models the decisions of the defenders, and the internal category, which detects cyber-attack scenarios based on a given protection strategy. The choice of the optimal model for forecasting and evaluating critical infrastructure is the most important arm for the smooth and uninterrupted operation of the infrastructure. Using general models of future predictions and troubleshooting offers analysis and calculations of various ways and procedures using data collected in different methods. It presents results that are only sometimes accurate by failing to draw correct conclusions. The use of multiple models of predictions provides several outcomes and more ways for a comprehensive understanding of the issues. The RIMF model may improve identifying security practices connected to malicious attacks, systems, and multiple targets. Using models that are not ideal or insufficient to capture the problem may lead to inadequate application of security strategies and fail cyber-attack and system breaches.

The central part of this article consists of two sections. Section 2 describes the algorithm and how it can be used to identify vulnerabilities in the systems and implement cyber-security by applying best practices. In Section 3, critical infrastructure objects will be analysed to verify the algorithm's operation described in the second section.

2. Review of literature

The issue of security is one of the important moments of the modern world, which has been discussed more than once and will be discussed in the future since not only the economic or political state of the country but also the people depend on it. There are many articles, guides and methods you need to do to protect yourself, your property and your finances. Nevertheless, only a few ways can determine a particular system's safety. Much attention is paid to methods that, through data analysis and specific calculations, can determine the probability of attacks and the level of protection of systems. In their publications and articles, scientists describe the use of various models to establish a particular object's security level or to determine the likelihood of an attack on it. Recently, scientists have been actively studying and describing in their works the possibilities of using one of these methods in different areas, called the r-Interdiction Median Problem with Fortification method (Zhang, Li & Jin, 2022).

For a very long time, sources of risk, due to which you can lose not only the object but also the supply of goods and services, due to natural causes, such as floods and fires, and man-made causes, such as terrorism and military operations (Church, Scaparra & Middlenton, 2004), have attracted attention. In 689 BC, the king of Sennacherib built a dam on the Euphrates River to deliberately create a manufactured disaster by flooding the city of Babylon (Church & Scaparra, 2005). In turn, the military tried to identify critical points in the supply chain, the defeat of which would lead to delays or reduction in supplies to conflict zones (Church & Scaparra, 2005).

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

Critical infrastructure may be defined as those elements that, when lost, significantly disrupt the system's ability to perform its function. These elements can include transportation linkages (e.g. bridges, tunnels, rail, etc.), facilities (e.g. port terminals, production facilities, warehouses, operations centers, emergency response facilities, hospitals, etc.), critical stockpiles (e.g. smallpox vaccine, drugs, food, etc.), key personnel (e.g. water system operators) and landmarks that may contribute to loss of well-being. Grubesic et al. (2008) studied network survivability by calculating network connectivity given a specific node or link failure. These studies aim to study and identify critical components, not the reliability and safety of the entire system. For example, if one of the power supply facilities covering a large area fails, the remaining facilities will not have enough resources to provide electricity, which will disrupt the entire system (Azaiez & Bier, 2007; Su, Gao, & Zhang, 2022). Therefore, one of the research priorities is the development of methods for protecting critical infrastructure (Church, Scaparra, & Middlenton, 2004, Soto et al., 2015; Zhang et al., 2023).

Previously used mathematical models for identifying network vulnerabilities have focused on determining how the loss of one or more objects will affect the operation of the infrastructure. For early models of prohibitions, see a publication by Church, Scaparra and Middlenton (2004), "Identifying critical infrastructure: The median and covering facility interdiction problems". They provide a short list of previously developed models, systematized according their goals, types, special constraints and the main network model.

Deny models help to identify potential weaknesses in the system without optimising security. For example, how to understand which facilities should be strengthened or secured? All objects, if the security process is relatively inexpensive. However, what if resources are limited and security costs are high? It is not sure, then, that an object's security, defined as critical, can provide the most excellent protection against an intelligent antagonist (Scaparra & Middlenton, 2008). Therefore, the optimal interdiction depends on what needs to be strengthened to prevent the consequences as much as possible. For this, the assumption was introduced that resources are limited and only a part of objects can be protected. The fortification was necessary to expand the possibilities of applying the median r-prohibition model to things that should be protected and to minimise the impact of prohibitions on other objects (Church & Scaparra, 2005).

The r-Interdiction Median Problem with the Fortification method is based on the p-median system structure. The main task of which is to find the optimal solution by placing p objects in the network in such a way as to reduce the cost of their maintenance and delivery. Most studies use a game theoretic approach and formulate protection problems as bi-level defender-attacker models (Scaparra & Church, 2008; Xiao et al., 2019). Researchers studying two-level and three-level tasks have extended the prohibition models to include protection decisions.

They developed a maximum-minimum budget allocation model, which makes critical infrastructure more resistant to physical attacks. The researchers consider problems within budget constraints, maximising the minimum cost of a possible attack.

Analysing scientific articles describing the r-Interdiction Median Problem with the Fortification method, one can notice that the theory described in the publication by Church, Scaparra and Middlenton (2004) is taken as the basis for all calculations. Therefore, from all the studied articles (Higle, 2005; Berman, Krass, & Menezes, 2007; Liu, Fan, & Ordonez, 2009; Aksen, Piyade, & Aras, 2010; Jenelius, Westin & Holmgren, 2010; Akbari-Jafarabadi et al., 2017; Li, X., Kizito, & Paula, 2018; Roboredo, Pessoa, & Aizemberg, 2019) one was chosen for further research, which deals with attacks on critical objects. Only some scientific articles consider the possibility of using the method to integrate it into cyber strategy. Therefore, this article will analyse the methods of calculation and the results obtained, described in the article by Scaparra Liberation and Daskin (2011). According to the authors, this example can be used when creating a cybersecurity strategy.

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

3. The RIMF model

When forecasting infrastructure problems, it should be emphasised that a probability assessment should be carried out. The use of a highly reliable problem-solving model and the use of the best cyber-security practices must be implemented to design strategies against multiple numbers and vectors of attack, even when the probability distribution and intruders' behaviour are unknown.

Therefore, the information from conducting forecast studies and proposed solutions will not only focus on high-probability scenarios but will be more general in predicting all possible future scenarios.

Forecasting will focus on comparing parts of the infrastructure by invoking stochastic optimisation methods. This will be achieved by making the best use of security resources or energy management information systems, significantly limiting the extent of the damage. Creating proprietary security algorithms that leverage the capabilities of the infrastructure in this way could motivate the design and creation of more secure equipment, the result of innovative applications, and a significant reduction, if not elimination, of the risk of system breaches within critical infrastructure.

Vulnerability assessment and risk analysis models for cyber-attacks that are either human-induced are used to design plans for security policy upgrades or critical infrastructure upgrades, as well as an understanding of vulnerable systems that need upgrades. The study considers a range of data, including infrastructure users, how they access the equipment, the communication networks, the way of communication and the processes performed. The main concern is optimising the entire infrastructure to make it more efficient and secure. A well-known model for capturing vulnerabilities in systems that are a part of critical infrastructure is the r-Interdiction Median Problem with Fortification (RIMF**)** model. The model is used to identify vulnerabilities in the systems and to implement security practices by applying optimal solutions provided that managers of the model know in advance and try to evaluate the vulnerabilities of the model. Both are analysing and capturing problems is a process that distorts reality, as it captures malicious actions, cyber-attacks, and physical attacks on infrastructure, which without the use of predictive models would be uncertain thoughts about the future, which with time would lead to uncertainty and might repeat in the future without a clear understanding of events that would follow.

Over time, the use of the RIMF model has been expanded and upgraded as a stochastic component has been added, which can examine system problems against a range of cyber-attacks, which vary between one and a maximum number of R. In this way, every resulting output is associated with some probability, while for the minimisation of false or incomplete result which has a large exclusion from the actual data of the problem, so to minimise the loss of the worst case means to treat, through protection, all interference that further damages the systems so that only the least harmful ones can occur. A prediction model like RIMF is not infallible, it is likely to produce data that does not exactly address the problems and weaknesses, which is directly related to future cyber-security and physical protection strategies that need to be implemented in critical infrastructure. Nevertheless, the model tends to identify with a high degree of precision future cyber-attacks and physical disasters. The model identifies optimal protection strategies that are considered satisfactory by correlating them with the number of problems. The design of the cyber and physical security analysis of critical infrastructure should take into account to a large extent the results of such studies, which often do not significantly deviate from their predictions, thinking that not all data may always be relevant, but something which is not related to problematic use or the lack of usefulness of the prediction model, but is often due to limited input such as critical historical data that may have been omitted.

Fortifying application is considered necessary to minimise the result's loss of accuracy and address the difficulties affecting the system under consideration. This phenomenon is called S-RIMF. RIMF can list all the interference in critical infrastructure and capture level by level the problems with the characteristic repressions of possible

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

obstructions (r) and installations (P). The model works as follows: Define with H_r where H is the obstruction points in the premises (r). Each obstruction point H is equivalent to a cyber-attack or a general threat, while l_h denotes all obstructions to critical infrastructure. C_h captures correlations with interference standards, (h) represents the cost of systems when facilities (L_h) are inactive. Standard (h) is presented as covered if on the premises I_h is enhanced.

The barrier model relates exclusively to unprotected critical infrastructure. The worst-case scenario and the loss of information should always be considered to take the necessary measures to protect critical infrastructure in such a way as to include disruptive attack patterns in the forecast analysis. The S-RIMF standards are as follows:

$$z_j = \begin{cases} 1, & If\ the\ location\ is\ enhanced \\ 0, & For\ any\ other\ case \end{cases} \quad (3.1)$$

$$y_h = \begin{cases} 1, & If\ the\ obstruction\ pattern\ h\ is\ covered \\ 0, & For\ any\ other\ case \end{cases} \quad (3.2)$$

The worst cost scenario is decoded by W_r, which (r) captures critical infrastructure. Therefore, the modelling will be as follows:

$$minZ^* = \sum_{r=1}^{R} p_r W_r \text{ , where} \quad (3.3)$$

$$W_r \geq c_h(1 - y_h) \forall h \in H_r, \forall_r = 1, \dots, R \quad (3.4)$$

$$\sum_{j \in I_h} z_j \geq y_h \forall_h \in H_r, \forall_r = 1, \dots, R \quad (3.5)$$

$$\sum_{j \in F} z_j \leq Q \quad (3.6)$$

$$z_j \in \{0,1\} \forall_j \in F \quad (3.7)$$

$$0 \leq y_h \leq 1 \forall h \in H_r, \forall_r = 1, \dots, R \quad (3.8)$$

Objectives of the above equation are the following:

- *The notation with (W_r) identifies the sum of costs in combination with operating costs.*
- *r = with the number of cyber-attacks compared to the loss value denoted by (W_r).*
- *H = number of critical infrastructures covered in combination with prohibition methods denoted by I_n.*
- *Q = symbolises the number of critical infrastructures, which shows increased protection.*
- *Confirmation of the variables that have been used.*

It is worth noting at this point that S-RIMF is complex and sometimes difficult to understand. Its complexity is directly related to the number of interference patterns combined with the number of critical infrastructures denoted by (P). As it is understood, the number of constraints and variables is related to the number of constraint patterns, then the prediction model is impractical and exceeds its implementation objectives; it is concluded that there is an improvement in uncertainty, which satisfactorily addresses the S-RIMF, which is a significant breakthrough in the field of protection modelling. If someone compares the RIMF and the S-RIMF will notice a considerable improvement in the prediction of cyber-attacks and general damages.

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

4. Practical application of the RIMF algorithm for critical infrastructure

The method described in Chapter 2 is widely used to solve problems of finding the optimal solution in many areas of activity. Numerous articles describe this method and are used to develop service systems, determine security methods, establish how much infrastructure can be subject to terrorist attacks, and optimally allocate funds and other resources to solve security issues.

In this article, we are discussing predicting cyber-attacks on critical infrastructure, the main focus was kept on research related to the study of strategies for protecting critical infrastructure from possible attacks, analysing probable failures and studying the design of reliable systems. A very good practical application of the RIMF model, with possible adjustments, additions and calculations, is described in the article by Scaparra Liberation and Daskin (2011) "Analysis of Facility Protection Strategies Against Uncertain Number of Attacks: The Stochastic R-Interdiction Median Problem with Fortification", which will be analysed in this Chapter.

The authors of the article "Analysis of Facility Protection Strategies against Uncertain Number of Attacks: The Stochastic R-Interdiction Median Problem with Fortification" use some geographical data in their research. More precisely, objects are located in the UK (150 objects) and USA (263 objects). Thus, to compare the results and test the method, 250 random evenly spaced objects were generated. All calculations were performed on a computer using the C ++ program. For optimisation, a special CPLEX 9.1 module allows to selection and set of the necessary parameters corresponding to the task. Using computer equipment and a particular program made it possible to reduce the calculation time and avoid errors associated with the human factor.

The study uses a large data set, so they were optimally divided into groups with a specific number of objects using the P-median method. The number of attacks (R) is not large, in the range from 2 to 5, and the value of objects that can be protected (Q) is proportional to the number of objects tested (P): 10%, 15% and 20%. As a result, the combination of parameters after the optimisation process looks like this (Table 1):

P	40	50	60
Q	4 6 8	5 8 10	6 9 12
R	2-5		

Table 1. Combination of parameters

The model identifies optimal protection strategies that are considered satisfactory by correlating them with the number of problems. To minimise costs (Wr), for each value of r, the program calculates a probability (pr), which helps to model the average value of attacks directed at a small number of objects. For these purposes, one of the formulas is used:

$$p_r = 2 * \frac{r}{R(R+1)} \quad or \quad p_r = 2 * \frac{R-r+1}{R(R+1)} \quad (4.1)$$

The results of the calculations are shown in Figures 1, 2 and 3 (Appendix I). As you can see, the first, second and third columns indicate the parameters P, Q and R. Further, the value of the optimal solution (Z *) for each data set and the average execution time of the algorithms. An asterisk marks those solutions that are not optimal for this data set. The last row shows the average running time of the algorithms for the entire data set.

Having analysed the studies described in the article "Analysis of Facility Protection Strategies Against Uncertain Number of Attacks: The Stochastic R-Interdiction Median Problem with Fortification" and the data obtained above, we can conclude that this method can also be used to find out the optimal solution for predicting cyber-attacks on critical infrastructure. As the data of the algorithm demonstrates, the number of objects and, of course, the number of analysed attacks influence the determination of the optimal solution. This method can be applied to

ISSN 2669-0195 (online) https://jssidoi.org/ird/
2023 Volume 5 Number 1 (March)
http://doi.org/10.9770/IRD.2023.5.1(6)

a specified number of attacks and an indefinite one, as in the example above. To achieve this, it is necessary to supplement the method with the definition of the upper and lower bounds. The exact number of attacks used in the calculations requires a long and detailed work of collecting data.

Using the results of the study described in the article "Analysis of Facility Protection Strategies Against Uncertain Number of Attacks: The Stochastic R-Interdiction Median Problem with Fortification", it is possible to improve the cyber prediction model for critical infrastructure, depending on what results have to be obtained. For example, by entering the maximum and minimum attack values for an indefinite number of threats, it is determined, in percentage terms, how far sub-optimal solutions are from optimal ones.

Conclusion

Unfortunately, the prediction models used to forecast future threats to critical infrastructure do not provide 100% accuracy, but they give essentially good forecasting for countering future attacks. More than just predicting threats from a single model is required, so more than one combination of prediction models is used, choosing a single threat prediction model can lead to ineffective future security strategies and result in sufficient security measures. Security control scenarios in critical infrastructure play an important role as for each scenario, an optimal security strategy has to be identified as determined by the prediction model. It should be noted that it might only be effective if there is a large number of interferences, and it may not be optimal if the foreseeable losses are small. The result will only be partially valid if the model identifies a low probability in combination with many failures. In implementing the model, the design of future security policies and critical protective infrastructure against multiple types of threats and cyber-attacks should be used, including those linked between multiple critical infrastructures and the elements should be considered. In addition, as mentioned above, the prediction models present an analysis that is approximately in line with the scenarios and data that were analysed. Based on the data that was evaluated, the potential threats, the extent of the damages and their costs are calculated. Finally, the prediction models and related tools are perfect for drafting the cyber-security strategy.

Cyber strategy is a long-term planning tool, and it needs to have future insight to develop. Developing cyber strategies is mandatory for planning technical capabilities to protect organisations from cyber threats. It is a necessary forecast for future cyber-attacks, which should be integrated into cyber security strategy.

Therefore, a method was analysed, using which it is possible to calculate not only the probability of a potential threat but also the amount of damage. Based on the data, their quantity and quality, it is possible to calculate for one separate object and several connected objects. Basically, the r-Interdiction Median Problem with Fortification (RIMF) method is used in logistics, economics, game development, the military, and more, but not in cybersecurity. Of course, there are many directions for future research related to the method and its application to ensure the safety of critical facilities. But, after analysing the application of the r-Interdiction Median Problem with Fortification (RIMF) method, the main task of this article is to decide whether it is possible to use it in practice, integrating it into a security strategy. Of course, using this method is possible and even necessary to properly plan the possibilities for protecting organisations from cyber threats. The practical application of this method will help improve the cyber strategy of critical infrastructure. By collecting and analysing information received about critical objects, their protection and attacks on them, in the future, improving the method, and using additional calculation formulas, will only enhance and strengthen cybersecurity.

References

Akbari-Jafarabadi, M., Tavakkoli-Moghaddam, R., Mahmoodjanloo, M., Rahimi, Y. (2017). A tri-level r-interdiction median model for a facility location problem under imminent attack. *Computers & Industrial Engineering*, 11, 151-165 https://doi.org/10.1016/j.cie.2017.10.003

Aksen, D., Piyade, N., & Aras, N. (2010). The budget constrained r-interdiction median problem with capacity expansion. *CEJOR Central European Journal of Operation Research*, 18, 269-291. https://doi.org/10.1007/s10100-009-0110-6

Almaleh, A., & Tipper, D. (2022). Risk-Based Criticality Assessment for Smart Critical Infrastructures *Infrastructures*, 7(1), Article Number 3 https://doi.org/10.3390/infrastructures7010003

Azaiez, N.V., & Bier, V.M. (2007). Optimal resource allocation for security in reliability systems. *European Journal of Operational Research*, 181, 2(1), 773-786. https://doi.org/10.1016/j.ejor.2006.03.057

Berman, O., Krass, D., & Menezes, M.B.C. (2007). Facility reliability issues in network p-median problems: strategic centralisation and co-location effects. *Operations Research*, 55(2), ii-397. https://doi.org/10.1287/opre.1060.0348

Bitirgen, K., & Filik, U. (2023). A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. *International Journal of Critical Infrastructure Protection*, 40, Article Number 100582 https://doi.org/10.1016/j.ijcip.2022.100582

Church, R.L., & Scaparra, M.P. (2005). Protecting critical assets: The r-interdiction median problem with fortification. KBS University of Kent.

Church, R.L. Scaparra, M.P., & Middlenton, R.S. (2004). Identifying critical infrastructure: The median and covering facility interdiction problems. Department of Geography, University of California, Santa Barbara. https://doi.org/10.1111/j.1467-8306.2004.00410.x

Grubesic, T. H., Matisziw, T. C., Murray, A. T., & Snediker, D. (2008). Comparative Approaches for Assessing Network Vulnerability. *International Regional Science Review*, 31(1), 88-112. https://doi.org/10.1177/0160017607308679

Higle, J.L. (2005). Stochastic programming: optimisation when uncertainty matters. Tutorials in Operations Research. https://doi.org/10.1287/educ.1053.0016

Jenelius, E., Westin, J., & Holmgren, J. (2010). Critical infrastructure protection under imperfect attacker perception. *International Journal of Critical Infrastructure Protection*, 3(1), 16-26. https://doi.org/10.1016/j.ijcip.2009.10.002

Li, X., Kizito, R., & Paula, T.I. (2018). An agent-based simulation framework for supply chain disruptions and facility fortification. Proceedings of the 2018 Winter conference. Date of Conference: 09-12 December 2018 https://doi.org/10.1109/WSC.2018.8632475

Liberatore, F., Scaparra, M.P., & Daskin, M. (2011). Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification. *Computers and Operation Research*, 38(1), 357-366. https://doi.org/10.1016/j.cor.2010.06.002

Liu, C., Fan, Y., & Ordonez, F. (2009). A two-stage stochastic programming model for transportation network protection. *Computers and Operations Researc*h, 36(5), 1582-1590. https://doi.org/10.1016/j.cor.2008.03.001

Parvasi, S.P. Tavakkoli-Moghaddam, R., Bashirzadeh, R., Taleizadeh, A.A., & Baboli, A. (2020). Designing a model for service facility protection with a time horizon based on tri-level programming. *Engineering Optimisation*, 52(1), 90-105. https://doi.org/10.1080/0305215X.2019.1577408

Roboredo, M.C., Pessoa, A.A., & Aizemberg, L. (2019). An exact approach for the r-interdiction median problem with fortification. *Rairo-Operations Research*, 53(2), 505-516. https://doi.org/10.1051/ro/2017060

Scaparra, M.P., & Church, R.L. (2008). A bilevel mixed-integer program for critical infrastructure protection planning. *Computers and Operation Research*, 15(2-3), 99-127, https://doi.org/10.1016/j.cor.2006.09.019

Snyder, L.V., & Daskin, M.S. (2005). Reliability models for facility location: the expected failure cost case. *Transportation Science*, 39(3), 289-441. https://doi.org/10.1287/trsc.1040.0107

Somogyi, T., & Nagy, R. (2022). Some impacts of global warming on critical infrastructure protection - heat waves and the European financial sector. *Insights into Regional Development*, 4(4), 11-20. https://doi.org/10.9770/IRD.2022.4.4(1)

Soto, R., Crawford, B., Vilches, J., Johnson, F., & Paredes, F. (2015). Heuristic Feasibility and Preprocessing for a Set Covering Solver Based on Firefly Optimization. In: Silhavy, R., Senkerik, R., Oplatkova, Z., Prokopova, Z., Silhavy, P. (eds) Artificial Intelligence Perspectives and Applications. *Advances in Intelligent Systems and Computing*, 347. Springer, Cham. https://doi.org/10.1007/978-3-319-18476-0_11

Su, Y.M., Gao, H.Y., & Zhang, S.B. (2022). Hybrid Resource Allocation Scheme in Secure Intelligent Reflecting Surface-Assisted IoT. *KSII Transactions on Internet and Information Systems*, 16(10), 3256-3274. https://doi.org/10.3837/tiis.2022.10.003

Tvaronavičienė, M., Plėta, T., Beretas, Ch.P., & Lelešienė, L. (2022). Analysis of the critical infrastructure cyber security policy. *Insights into Regional Development*, 4(1), 26-39 https://doi.org/10.9770/IRD.2022.4.1(2)

Xiao, Y., Zhang, P.Y., Zhang, S., Zhou, S., Chang, W., &. Zhang, Y. (2019). Dynamic gaming case of the R-interdiction median problem with fortification and an MILP-Based solution approach. *Sustainability*, 12(2), 581. https://doi.org/10.3390/su12020581

Zhang, J.T., Bagtzoglou, Y., Zhu, J., Li, B.K., & Zhang, W. (2023). Fragility-based system performance assessment of critical power infrastructure. *Reliability Engineering & System Safety* 232, Article Number109065 http://doi.org/10.1016/j.ress.2022.109065

Zhang, K.K., Li, X.P., & Jin, M.Z. (2022). Efficient Solution Methods for a General r-Interdiction Median Problem with Fortification. *Informs Journal on Computing*, 34(2), 1272-1290. http://doi.org/10.1287/ijoc.2021.1111

Zheng, K., & Albert, L.A. (2018). An exact algorithm for solving the bi-level facility interdiction and fortification problem. *Operations Research Letters*, 46(6), 573-578C. https://doi.org/10.1016/j.orl.2018.10.001

Funding: The research was partly financed by project “The Impact of Technological Progress of Industry 4.0 on the Development and Value of Industrial Production Sector”ITPI4, No 09.3.3-LMT-K-712-19-0037 (2014-2020 Measure No. 9 of priority 9 "Education of society and increasing the potential of human resources" of the action program of investments of EU funds)

Author Contributions: The authors contribute equaly; they have read and agreed to the published version of the manuscript.

Joana KATINA is a Dr. of Information Technologies. She works at Vilnius University as Assistant professor (Institute of Computer Science, Department of Computational and Data Modeling). Her main research areas are data modeling, algorithms and data structures.
ORCID ID: https://orcid.org/0000-0002-0715-1675

Tomas PLĖTA is an Advisor of the Regional Cyber Defence Centre, a subsidiary of the National Cyber Security Centre under the Ministry of National Defence of the Republic of Lithuania and PhD student at Vilnius Gediminas Technical University. His PhD topic is related to cyber security management for critical energy infrastructure. His research interests include information and data security, data protection, and industrial control system cybersecurity.
ORCID ID: https://orcid.org/0000-0002-5376-6873

Romualdas PETKEVIČIUS is a Director of the Regional Cyber Defence Centre, a National Cyber Security Centre subsidiary under the Ministry of National Defence of the Republic of Lithuania and a Master student at the Mykolas Romeris University. His Master thesis is related to cybersecurity management.
ORCID ID: https://orcid.org/0000-0001-7869-4098

Lina LELEŠIENĖ is a PhD student at the Mykolas Romeris University (e-mail: lelesiene.lina@gmail.com). Her PhD topic is related to cyber security management of e-health systems. Her research interests also included information security in banking, data protection, and cyber security issues.
ORCID ID: https://orcid.org/0000-0002-6822-9907

Make your research more visible, join the Twitter account of INSIGHTS INTO REGIONAL DEVELOPMENT:
@IntoInsights

This is peer-reviewed scientific journal https://jssidoi.org/ird/page/peer-review-policy

Copyright © 2023 by author(s) and VsI Entrepreneurship and Sustainability Center
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access