International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

An Empirical Paradigm on Cybersecurity Vulnerability Mitigation Framework

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
rohit.vallabhaneni.2222@gmail.com

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
doctorabhilashmaroju@gmail.com

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com.

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA.
sravanthi.dontu13@gmail.com

ABSTRACT

Current cybersecurity vulnerability assessment tools were developed in accordance with guidelines established by entities like the National Institute of Standards and Technology (NIST) and the United States Department of Energy. When assessing their facility's cybersecurity maturity, owners and operators of critical infrastructure frequently use frameworks like the NIST Cybersecurity Framework (CSF) and the cybersecurity capability maturity model (C2M2). These frameworks are great at finding vulnerabilities and doing qualitative cybersecurity analysis, but they don't help you get to the level of cybersecurity maturity you want by letting you prioritise how you fix those flaws. Cyber dangers pose a significant risk to businesses and are becoming more pervasive in our everyday lives. In this way, businesses may devise a strategy and set of guidelines by simulating a breach attack. But these strategies are based on experts' tacit knowledge. In response to this problem, the authors of this study suggest an automated and formal process for creating prioritised action plans to enhance environmental transparency. An experiment proving the validity of the proposed method was conducted, yielding consistent and applicable results to the tested scenario. Through testing against a real-world cyberattack that targeted industrial control systems at a critical infrastructure facility, this article presents a thorough architecture of CyFEr and demonstrates its application to CSF.

1. INTRODUCTION

In today's increasingly interconnected world, cyber technologies are having a profound impact on society, businesses, and economies. Cybercrime has also increased in tandem with the exponential development of internet use. The actuality of the COVID-19 pandemic has boosted online contact, which is the main reason for excessive use of web-based apps (Buil-Gil et al. 2021). Criminals online steal sensitive data and thwart legitimate financial transactions made by individuals, organisations, and governments through malicious web applications (Chigada and Madzinga 2021). Given this context, cybersecurity research has become increasingly popular among both academics and practitioners.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

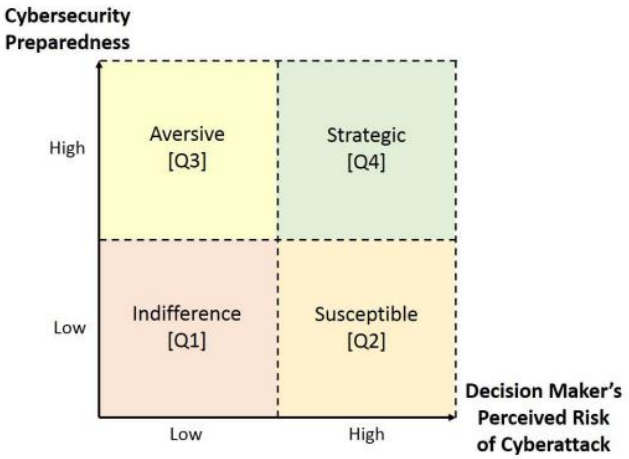

Figure 1. Cybersecurity Preparedness-Risk Taxonomy (CyPRisT).

This study used the CyPRisT to categorise small firms according to their cybersecurity postures for business continuity, and it also used the sample's cybersecurity preparation and decision makers' assessed risk of cyber-attack scores. The CyPRisT is a four-dimensional tool for gauging the perceived risk of cyber-attacks on small businesses. Its dimensions include indifference (Q1), vulnerable (Q2), aversive (Q3), and strategic (Q4). These dimensions provide benchmark scores for cybersecurity readiness. Protecting systems and activities from unauthorised electronic attacks is what cybersecurity is all about according to this study. Cybersecurity is the process of protecting computer systems, servers, mobile devices, data, and other electronic equipment from intrusion, according to Conteh (2021). Businesses, mobile devices, and information systems and networks are all vulnerable to cyberattacks, so it's clear that cybersecurity is important in many different settings. With a wide array of cyber threats emerging from many sources, it is critical to improve cybersecurity systems to identify, stop, and react quickly to harmful attacks (Horgan et al. 2021).

Attacks on computer systems, networks, infrastructure, servers, and other information resources (such as mobile devices and personal PCs) are known as cybercrime. Disabling systems, stealing information, and making the overall system inefficient are the main goals (Lallie et al. 2021). Malware, phishing, and ransomware are just a few of the strategies employed in cyberattacks. This highlights the need for continuous study into the development of security systems capable of detecting and preventing various breaches.

Even though small firms face the same cybersecurity risks as major corporations, small-scale traders often believe they are not vulnerable because of their size and anonymity (Banham 2017). (R. Manikyam. 2019) That isn't the case, though, because cybercriminals can now concurrently target hundreds—if not thousands—of small-scale enterprises thanks to rising automation (Joel 2021). Fuentes (2020) claims that small enterprises typically lack the resources to invest in cybersecurity, are less knowledgeable about potential attacks, and have less robust technology defences. Because of this, hackers find them easier targets than larger businesses.

2. LITERATURE REVIEW

This research looked at the effects of cybersecurity risks and weaknesses on migrant traders from Africa who operate on a smaller scale in Southern Africa. Entrepreneurs identified as small-scale African migrant traders are those whose businesses are not large enough to warrant regulation and who employ a small number of people. Operating at a micro level, they frequently engage in low-volume trades amongst themselves and their clients. According to Croke et al. (2020), these merchants have taken use of internet commerce to boost their economic activities, thanks to the expansion of information technologies and the improvement in worldwide connectivity. (Ramya Manikyam. 2016).
Ransomware, malware, spam, and harmful websites are some of the ways used. Additionally, attackers are utilising COVID-19 misinformation as a new tool to undermine financial institutions and enterprises worldwide. In order to get access to computer systems, networks, data servers, and mobile devices, hackers utilise false news and misinformation as a bait (Interpol, 2020).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Thus, cybersecurity research started to gain momentum as both academics and practitioners aimed to create methods and technologies that could identify and thwart cyber threats before they could cause system failure. The change in focus towards health and other measures to control the spread of COVID-19 has been exploited by cybercriminals (Carías et al. 2020). Cyber hazards have affected companies of all sizes that have conducted online operations over unreliable and unprotected Internet connections (Rao et al. 2021).

Exposure to cybercrime is on the rise in tandem with the degree to which international trade is becoming linked (Ruvin et al. 2020). The majority of cyberattacks and threats, however, are carried out by humans. This suggests that entrepreneurs are vulnerable to cyberattacks due to human behaviour and ethical conduct (Pandey et al. 2020). Since small-scale traders have embraced remote work styles to boost their economic operations, it is crucial to explore the vulnerabilities they face while doing so. This is because small-scale traders are more connected to the world and have access to more information than ever before.

3. METHODOLOGY

A gap analysis-performing architecture is present in both C2M2 and CSF. Which is why this study makes use of the same modified design. However, prioritised vulnerability analysis is not something that CSF or C2M2 are capable of doing. A "multi-scenario and criteria based" vulnerability analysis will be conducted as part of this planned research to help with mitigation techniques. Following the completion of the cybersecurity maturity model and framework's foundational evaluation, a series of rational procedures will be carried out to accomplish this. The cybersecurity objectives and target outcome dictate the order of the computations. Hierarchical execution of several processes is involved in prioritised gap analysis (PGA), as shown in Fig. 2. After the cybersecurity objectives and ranking criteria have been defined, the CyFEr framework employs a multi-tiered constraint-based optimisation strategy to eliminate unnecessary solution structures. After the filtering process is complete, the CyFEr framework starts the PGA to evaluate the cybersecurity posture and effectively measure the effort needed to achieve the desired state. PGA accomplishes this by calculating the scalar values of the solutions based on all the changes in the states of the security controls after analysing all the discovered cybersecurity postures (filtered solutions). The ranks of the solutions are then determined by the scalar values.

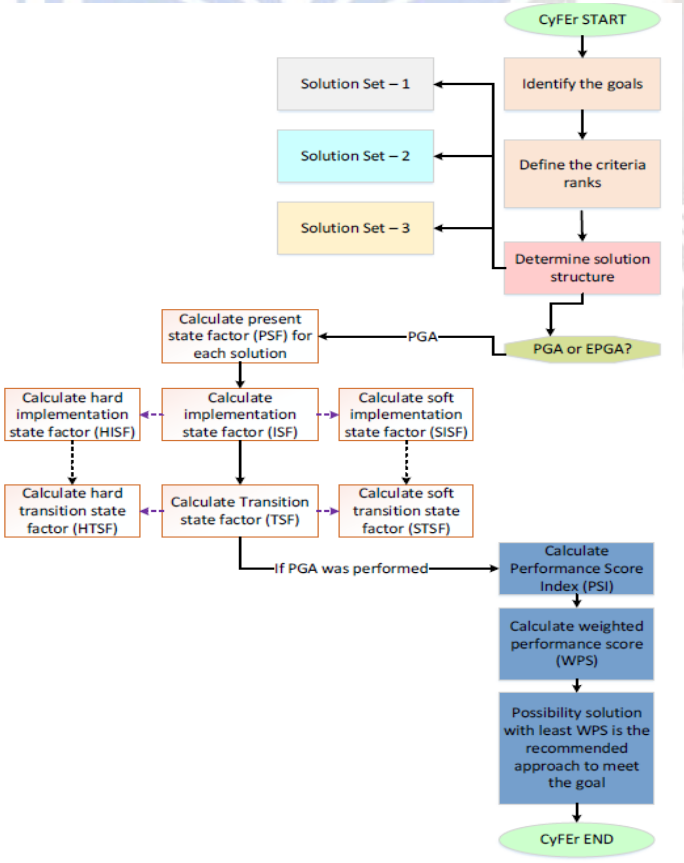

Fig. 2. Workflow of prioritized gap analysis

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

A. Step – 1: Determine the Objectives The desired cybersecurity maturity can be defined when the objective has been identified. Given the present state of 50% maturity (please note that any control in states 3 or 4 {largely or fully implemented} is deemed a mature control), the final maturity should be at 70%. This is an illustration of the desired maturity.

B. Step – 2: Classify the Criteria The term "criteria" refers to all the potential qualities that are unrelated to the ultimate result. Together with the objective, the desired standards will be laid down. Criteria can be expressed as follows: "along with the intended state, a specific subdomain (for instance, access control) is ranked as 1, asset management as 2, and so on."

Implementation Solution: The following formulation makes the aforementioned constraint a reality.

Algorithm – 1: Constrain – 1 (Solution Set – 1)

$1: s \in S_1^{future}$ if $s \notin S_1^{present}, S.T$

$2:$ while $M_{net} \le x\%$

$3:$ for $C_i, \forall C_i \in \left\{C_{Total}^{Ranked}\right\}, where\ C_{Total}^{Ranked} = \{C_1, C_2, ..., C_i, ..., C_n\}; n = 23$

$4:$ while $M_i^{net} \le x\%$

$5:$ $\forall Q_n^{MIL1}, Q_i^{MIL1} \rightarrow S_{\{3\|4\}}$

$6:$ Then, $\forall Q_n^{MIL2}, Q_i^{MIL2} \rightarrow S_{\{3\|4\}}$

$7:$ Then, $\forall Q_n^{MIL3}, Q_i^{MIL3} \rightarrow S_{\{3\|4\}}$

First, the CyFEr framework incorporates the rank-weight methods rank sum, second, rank reciprocal rank, third, rank exponent, and fourth, rank order centroid. What follows is a discussion of the formulations and detailed analysis.

Rank Sum (RS): In the case where there are n criteria, the rank of criterion i is determined by:

$$W_i^{RS} = 2(n - r + 1)$$

Reciprocal Rank: This is the case for n=r criteria, where i is a criterion of rank r:

$$W_i^{RR} = \frac{1}{r}$$

We find the normalised weight of criterion i by doing the following:

$$W_{i|norm}^{RR} = \frac{W_i^{RR}}{\sum_{i=1}^{n} W_i^{RR}} = \frac{\left(1/r\right)}{\sum_{i=1}^{n} W_i^{RR}}$$

Rank Order Centroid: The formula for C of criterion i of rank r is given for n number of criteria:

$$W_i^{ROC} = W_{i|norm}^{ROC} = \frac{1}{n}\sum_{j=i}^{n}\frac{1}{j}$$

Prioritizing Actions to Improve the Detection

Figure 3 shows the proposed technique of this research, which uses the outcomes of a breach assault simulation to provide a list of suggestions for cyber threat visibility enhancement, either for all threats or for a specific subset of them. After this set of suggestions has been finalised, the method will use a decision-maker-selected MCDA approach to prioritise the control items in Table 3, which are directly related to the ATT&CK procedures that will be put into execution. Items such as the MITRE ATT&CK data sources into methodologies, the NIST Common Security Framework, CIS, or ISACA COBIT might be used as control items.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

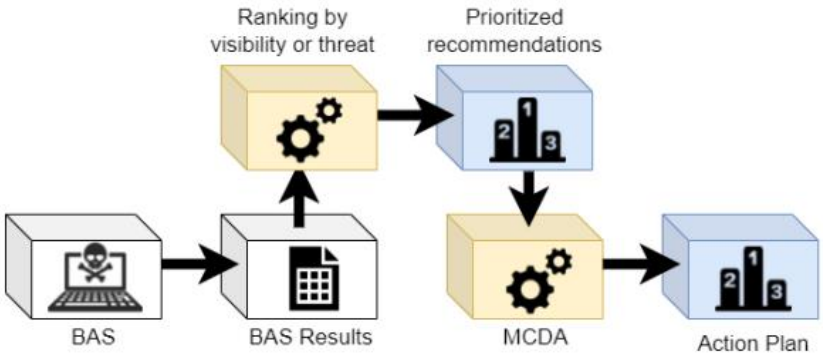

Figure 3. Prioritizing process based in BAS results and MCDA methods

The suggested procedure includes importing the BAS results, which then produce a list of suggestions to improve the security posture according to the visibility seen in the BAS exercise. Afterwards, an action plan with the control items prioritised by an MCDA method is chosen and put into action.

4. RESULTS AND DISCUSSION

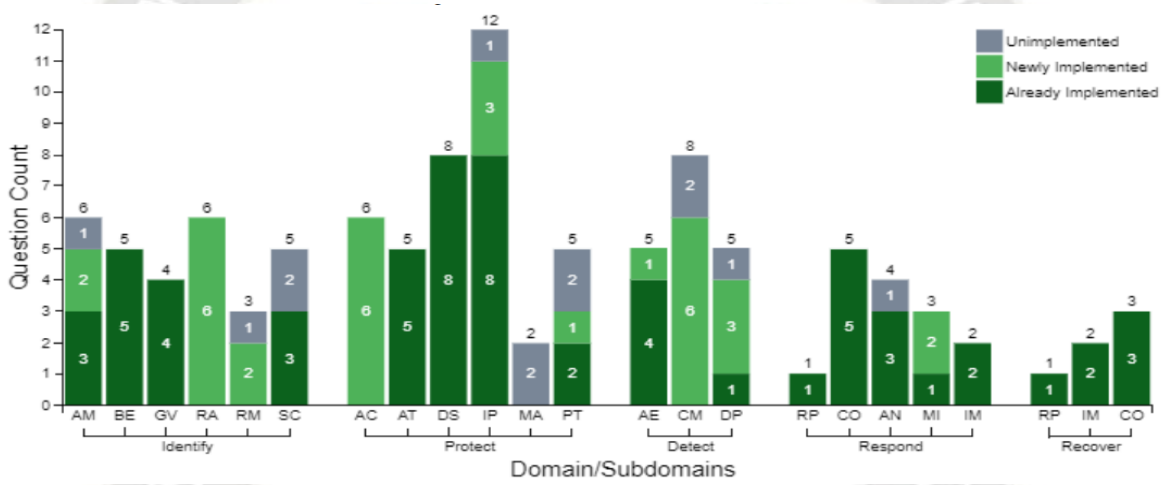

Fig. 4. Depiction of impacted controls for PGA Soft's solution

Figure 4 displays the control state transitions that were impacted by the solution that was found.

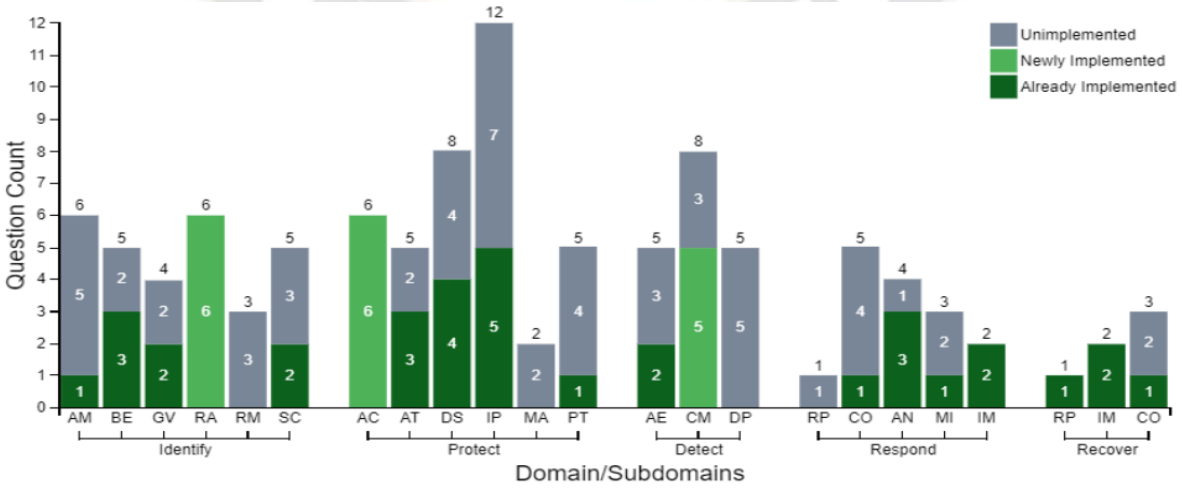

Fig. 5. Depiction of impacted controls for PGA Hard's solution

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

Figure 5 shows that there were fewer control transitions than in Figure 4, but that the controls that did change achieved the maximum acquirable state, which is Fully Implemented.

Table 1. CIS controls prioritized by 3 diferent MCDA methods

#	TOPSIS	WASPAS	ELECTRE	#	TOPSIS	WASPAS	ELECTRE
1º	4.1	4.1	4.1	**29º**	18.2	16.1	16.1
2º	4.7	18.2	11.2	**30º**	11.1	4.7	4.7
3º	4.10	11.2	11.3	**31º**	11.2	16.8	4.10
4º	5.2	11.3	11.4	**32º**	11.3	4.10	5.2
5º	6.3	11.4	11.5	**33º**	11.4	5.2	6.3
6º	6.4	11.5	4.2	**34º**	11.5	6.3	6.4
7º	6.5	4.2	4.5	**35º**	4.2	6.4	6.5
8º	3.1	4.5	6.1	**36º**	4.5	6.5	3.1
9º	5.3	6.1	6.2	**37º**	6.1	3.1	5.3
10º	5.4	6.2	13.4	**38º**	6.2	5.3	5.4
11º	5.5	13.4	7.1	**39º**	13.4	5.4	5.5
12º	6.8	7.1	7.2	**40º**	7.1	5.5	6.8
13º	2.5	7.2	7.3	**41º**	7.2	6.8	13.8
14º	2.6	7.3	18.2	**42º**	7.3	2.5	2.5
15º	16.13	7.4	11.1	**43º**	7.4	2.6	16.8
16º	18.3	7.5	7.4	**44º**	7.5	16.13	2.6
17º	18.5	10.5	7.5	**45º**	10.5	18.3	16.13
18º	3.12	3.3	10.5	**46º**	3.3	18.5	18.3
19º	4.4	9.2	3.3	**47º**	9.2	3.12	18.5
20º	4.8	14.1	9.2	**48º**	14.1	4.4	3.12
21º	7.6	14.3	14.1	**49º**	14.3	4.8	4.4
22º	7.7	16.1	14.3	**50º**	16.1	7.6	4.8
23º	12.2	16.9	16.1	**51º**	16.9	7.7	7.6
24º	12.8	9.3	16.9	**52º**	9.3	12.2	7.7
25º	13.3	5.1	9.3	**53º**	5.1	12.8	12.2
26º	13.8	14.9	5.1	**54º**	14.9	13.3	12.8
27º	16.8	15.7	14.9	**55º**	15.7	13.8	13.3
28º	16.1	11.1	15.7	**56º**	8.3	8.3	8.3

The next step in developing an action plan is for the decision maker to select an MCDA approach. Since this experiment's overarching goal is to provide a proof of concept, we opted to use three widely-used and diverse decision-making methodologies: TOPSIS, ELECTRE II, and WASPAS. Table 1 is a compilation of the spreadsheet output produced at the conclusion of the experiment, which is the consequence of applying these approaches in accordance with the decision matrix format described to create action plans based on CIS controls.

CONCLUSION

Models, methodologies, and tools for conducting cybersecurity vulnerability assessments are highly effective in locating security holes in a building, system, or network. These technologies, however, are unable to take user input and generate a mitigation strategy backed by mathematical and logical principles. The technique and architecture given in this study can be used with several well-established vulnerability analysis frameworks, including C2M2, CSF, and RMF. A real-world cyberattack was also used to test the proposed mitigation mechanism in this article. It was clear from the attack-based analysis that CyFEr, the mitigation approach, conducted an efficient study through thousands of solutions to achieve maturity. Aiming for a certain level of cybersecurity maturity, CyFEr also found the best possible solutions that could satisfy all user needs.

REFERENCES

1. Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. 2021. Cybercrime and shifts in opportunities during

COVID-19: A preliminary analysis in the UK. *European Societies* 23 (sup1): S47–S59.

2. Chigada, Joel, and Rujeko Madzinga. 2021. Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management* 23 (1): 1–11.
3. Conteh, Nabie Y. 2021. The dynamics of social engineering and cybercrime in the digital age. In *Ethical hacking techniques and countermeasures for cybercrime prevention*, 144–149. Hershey, PA: IGI Global.
4. Horgan, Shane, Ben Collier, Richard Jones, and Lynsay Shepherd. 2021. Re-territorialising the policing of cybercrime in the post-COVID-19 era: Towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology* 11 (3): 222–239.
5. Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 105: 102248. https://doi.org/10.1016/j.cose.2021.102248
6. Banham, Russ. 2017. Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy* 224 (1): 75.
7. Joel, Witts. 2021. The top 5 biggest cyber security threats that small businesses face and how to stop them. https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/. Accessed 27 Oct 2022.
8. Fuentes, M.R. 2020. An investigation into the current condition of underground markets and cybercriminal forums', Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digitalthreats/trading-in-the-dark. Accessed 24 Aug 2022
9. Croke, Kevin, Maria Elena Garcia Mora, Markus Goldstein, Edouard Romeo Mensah, and Michael O'Sullivan. 2020. Up before Dawn: Experimental evidence from a cross-border trader training at the Democratic Republic of Congo Rwanda Border. *Rwanda Border (January 27, 2020). World Bank Policy Research Working Paper* (9123).
10. Interpol. 2020. COVID-19 cyberthreats. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. Accessed 24 Aug 2021.
11. Carías, Juan Francisco, Marcos RS. Borges, Leire Labaka, Saioa Arrizabalaga, and Josune Hernantes. 2020. Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access* 8: 174200–174221
12. Rao, Sanjeev, Anil Kumar Verma, and Tarunpreet Bhatia. 2021. Evolving cyber threats, combating techniques, and open issues in online social networks. In *Handbook of research on cyber crime and information privacy*, 219–235. IGI Global. https://doi.org/10.4018/978-1-7998-5728-0.ch012
13. Ruvin, Oleksandr, Nataliia Isaieva, Larysa Sukhomlyn, Kateryna Kalachenkova, and Nataliia Bilianska. 2020. Cybersecurity as an element of financial security in the conditions of globalization. *Journal of Security & Sustainability Issues* 10 (1): 175–188.
14. Pandey, Shipra, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. 2020. Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing* 13 (1): 103–128
15. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
16. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama