THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

Role of Cybersecurity Legal Frameworks in Shaping the Risk Preparedness of the Telecommunication Sector in Safaricom Head Office, Nairobi, Kenya

Ruth Kamau
Researcher, Department of Peace and International Studies, Daystar University, Kenya
Justus K. Musya
Lecturer, Department of Peace and International Studies, Daystar University, Kenya

Abstract:
The role of cybersecurity legal frameworks for assessing risk preparedness in the telecommunications industry is crucial to protecting sensitive information and guaranteeing the resilience of digital infrastructure. To investigate how legal frameworks affect the risk preparation tactics used by the massive telecom company, this research employs the Safaricom Head Office in Nairobi, Kenya, as a case study. The study adopts a descriptive methodology to thoroughly explore and describe the current cybersecurity legal landscape, including its conceptualization and subsequent impact on risk management within the company. This study is significant because of the rising reliance on digital technologies and the frequency and sophistication of cyber threats. Because the telecommunications sector is an essential backbone for many sectors, knowing the legal frameworks governing cybersecurity is critical to guaranteeing the reliability and security of communication networks. This includes determining how well Safaricom's cybersecurity policies correspond with regulatory requirements, identifying any gaps, and investigating compliance concerns. The study aims to gain a thorough understanding of the relationship between legal frameworks and risk management strategies, ultimately contributing to the improvement of cybersecurity practices in the telecommunications industry.

Keywords: *Cybersecurity, risk preparedness, legal frameworks, Safaricom head office, regulatory requirements, telecommunications industry*

1. Introduction

The telecommunications industry is a key component of international communication networks in a time when digital connectivity governs the world. The dependability and security of these networks are critical to the operation of numerous industries and the overall well-being of society (Cariolle, 2021). However, with the rising frequency and sophistication of cyber assaults, protecting sensitive data and guaranteeing the resilience of digital infrastructure have become critical problems. The cybersecurity legal frameworks in question include a wide range of laws, regulations, and standards aimed at mitigating the rising threats in the digital realm (Bechara & Schuch, 2021). These frameworks not only set the constraints within the organization's function but also significantly impact how they approach risk mitigation and preparedness.

The problem is that the cybersecurity threats that the telecom industry faces are complicated and constantly changing, and the legislative framework that aims to solve these threats exacerbates the problem. Moreover, indigenous leadership research may look into leadership styles and methods founded in African cultural contexts. If the findings stress teamwork, community engagement, and a sense of shared wealth, they may be consistent with Kenya's or other African countries' broader national development goals (Musya et al., 2023). Safaricom, as a key player in Kenya's telecommunications sector, is an appropriate case study for investigating how legal frameworks influence risk management techniques within the business (Muthuri et al., 2022). The primary goal is to understand how Safaricom navigates the complex legal landscape, corresponds to its cybersecurity policies with regulatory requirements, and addresses the obstacles to maintaining compliance.

The potential for significant ramifications should the security of these networks be compromised underscores the importance of researching cybersecurity legal frameworks and risk preparedness strategies. This research is not limited to Safaricom; it also benefits the larger telecommunications sector and policymakers who aim to strengthen the cybersecurity posture of critical infrastructure.

2. Background

The telecommunications industry has experienced a revolutionary transition, emerging as a crucial element of the global digital economy. The sector's role in supporting these activities has grown increasingly important as societies

depend more and more on interconnected networks for information exchange, business, and communication (Imamov, 2021). However, the explosive growth of digital communication has also brought with it currently unheard-of difficulties, especially concerning cybersecurity. As the main means of data transmission, the telecommunications sector is particularly vulnerable to cyber threats, which can take the form of sophisticated cyber espionage or illegal access and data breaches.

Governments and regulatory agencies have implemented a framework of laws and regulations aimed at protecting the integrity and confidentiality of digital communications in response to the growing cyber dangers (Safitra et al., 2023). These legal frameworks for cybersecurity include a wide range of rules, guidelines, and standards that specify the actions that companies need to take to strengthen their cyber defences. These policies in Kenya, like in many other jurisdictions, are intended to protect sensitive information while simultaneously ensuring the uninterrupted and secure operation of essential infrastructure (José Zapata Campos et al., 2023). Furthermore, (Musya et al., 2023) suggest that effective governance techniques and indigenous leadership principles may have some similarities. Understanding these synergies may provide insights into how indigenous leadership philosophies might be integrated into governance structures, thereby impacting the development and implementation of cybersecurity legal frameworks in the telecoms sector.

With its main office located in Nairobi, Safaricom is a major participant in the Kenyan telecom market, offering various services ranging from financial transactions to mobile communication. As the digital landscape changes and cyber-attacks become more sophisticated, companies like Safaricom need to navigate the complex legal terrain governing cybersecurity. To prevent and address possible cyber dangers, the organization must abide by these regulations and successfully incorporate them into its risk management strategies (Elert & Henrekson, 2021). The effectiveness of these legal mechanisms in influencing risk preparedness measures inside Safaricom and comparable corporations has important consequences for the security and dependability of telecommunications infrastructure. Understanding how Safaricom conceptualizes and addresses the issues created by cybersecurity legislation is critical for improving the telecoms industry's overall resilience in the face of a constantly shifting threat scenario.

3. Theoretical Framework

Securitization theory was originally developed by Ole Wæver in 1995 and was later improved by Barry Buzan 1998, a researcher at the Copenhagen School of Security Studies (Stritzel, 2014). The theory provides an understanding of the concept of securitization by arguing that the definition of security is based on the subjective aspect rather than the objective aspect (Buzan et al., 1998). This implies that transnational crimes are a subject of securitization as they pose security threats not only to individuals and organizations but also to the state. The theory also assumes that there are choices involved in deciding which issues are to be characterized as security threats and which political issues constitute extreme security issues that are labeled as dangerous and need to be urgently addressed (Buzan et al., 1998).

Further, other researchers from the Copenhagen School of Security Studies indicate that securitization methods are a methodical way to evaluate the security needs of the state by ranking the identified areas of security concern in order of importance (Balzacq & Guzzini, 2015). Aradau (2018) argued that the national security departments in most countries are ignorant of the need to broaden the focus of national security studies to include cyber security. The capability of the military, who are well-aware and often use physical means and measures to fight against terrorist attacks, should be integrated with the modern security systems available to protect the citizens of a country. Moreover, as the mechanisms and strategies used by terrorist groups to attack their targets have shifted to the use of modern technologies, the national security units and organization security units should also advance to the available modern cybersecurity solutions (Guzzini, 2011). This will help promote better partnerships between the national security unit and the specific counter-terrorism units in the fight against emerging crimes (Stritzel, 2014).

On the other hand, Howell and Richter-Montpetit (2020) improved the definition of security to include referent objects other than the state only. The reference objects involve understanding first the targeted people who are provided with security, those who provide security, and the purpose of providing security. This will play an essential role in helping the state authority, and policymakers understand the urgency of addressing the security issue and the measures to be taken to do so (Léonard & Kaunert, 2010). Further, Ngare (2018) argues that as the national security authorities conduct the national security needs assessment, they should also identify the areas where campaign awareness programs should focus first, then develop strategies for how these campaigns will be designed and implemented and coordinate ad-hoc efforts of different stakeholders. In the case of cybersecurity, the study suggests that the audience of the campaigns should prioritize all internet and smartphone users, from vulnerable students and young children to adults, employees, and board members of SMEs, industries, and delicate public offices.

Additionally, Bada, Von Solms, and Agrafiotis (2019) employed the securitization theory to outline the essential goals of cybersecurity awareness programs as being to communicate the risks from cybercrime, illustrate the need for better security controls and practices and the need to establish a chief information security officer (CISO). Therefore, this theory will apply to the study as it emphasizes the need for the national security unit to show more concern for the emerging issues of cybersecurity that include cyber terrorism and the need to adopt modern technological measures to fight against cyber threats and cyber terrorism (Burton & Lain, 2020). It also encourages partnerships between the national security unit and other stakeholders in promoting campaign awareness programs to train and educate people on cybersecurity and the risk measures that are involved.

4. Conceptualization

In India, due to the huge loss of data in large quantities through cybercrimes, its government enacted the Information Technology Act 2000, whose purpose was to prevent any type of crime directed towards cyber security. Additionally, several laws were amended, including the penal code and the Evidence Act, to strengthen the law in fighting against cybercrimes (Sultan et al., 2022). According to Kosseff (2019), the United States has various cyber security laws in the state and federal statutes, regulations binding guidelines, and court-related rules that are directed towards data security privacy and other matters of cyber security because in the US no single cyber security law applies to all the cybercrimes and incidences that take place.

In Africa, the African Union (AU) adopted on 27th June 2014 the AU Convention on Cybersecurity and Personal Data Protection 2014, which is primarily focused on electronic transactions, personal data protection, and cybercrimes. Further, the supplementary act A/SA.1/01/10 on personal data protection for Economic Community of West Africa states (ECOWAS), and the Data Protection Mode Law 2012 for the Southern African Development Community (SADC) came into play, not forgetting the East Africa Community (EAC) legal framework for cyber laws 2008 and adopted in 2010, (Makulilo, 2016). All these legal frameworks were brought forthwith for the member states to adopt them by the international data privacy standards.

However, according to the United Nations Conference on Trade and Development, the adoption of cyber security policies and regulations across Africa stands at 72 percent, which is the lowest across the globe, the reason being that only 39 out of the 54 African countries have cyber security legislation, 2 other countries are still developing the legislation, while 13 countries have not yet started the process of drafting the cyber security legislation. (UNCTAD, 2021). However, in 2019, the EU European Union teamed up with the ECOWAS Commission to begin the West African Response on Cyber security and Fight against cybercrime (OCWAR C) and adopted a regional cybercrime and cyber security strategy that is aimed at solving the increasing levels of cyber threats in the continent. (Ajijola & Allen, 2022).

The Kenyan government 2014 developed the National Cybersecurity Strategy, which highlights the country's cybersecurity posture in a way that facilitates cybersecurity awareness and fostering information sharing and collaboration among the relevant stakeholders. The Computer Misuse and Cybersecurity Act 2018 and the Kenya Information and Communication Amended Act are all in place to deal with cybercrimes (UNESCO, 2020). Further, the CAK has an established computer incident response team (CIRT) whose mandate is to coordinate national cyber security and reported cybercrimes (Mitullah, 2022).

Therefore, even with the counter-terrorism measures already put in place, the telecommunication sector still needs to enhance its cyber-security systems and increase its level of risk preparedness, as cybercriminals are daily inventing new ways of penetrating and compromising their systems to their advantage.

In a study by Gopal and Maweni (2019), comprehensive knowledge is generated on the level of cybercrime preparedness of the BRICS (Brazil, Russia, India, China, and South Africa) countries. The data were collected through a discussion of the literature and media reports that have been published on the subject and through the in-depth research of some important policy texts that control the cybersecurity frameworks in the BRICS countries. According to the extensive content analysis carried out, the study indicated that the most prominent strategic approach used by BRICS countries was digital infrastructure development, legal policies, economic issues, and social and cultural perspectives. However, the study advocated that the BRICS Think Tanks Council (BTTC) should aim to jointly develop policy initiatives while maintaining sovereignty to play a more prominent role in the global context.

Woods and Simpson (2017) examined the influence of cyber insurance policies on cybersecurity in the telecommunication industry in the US. The study carried out a systematic qualitative analysis of the underwriting processes for cyber insurance. The findings of the study disclosed that the main challenge that insurance companies offering cyber insurance coverage encounter is a lack of historical and credible data on cyber insurance, which can allow them to make better decisions about loss expectations. (Musya et al., 2023) advocate that cultural considerations play an extensive role in decision-making and risk management. Understanding how cultural aspects intersect with legal frameworks may provide a nuanced perspective on policy implementation and organizational tactics in the context of Safaricom's cybersecurity and risk preparedness studies. This is because cyber insurance is a relatively new insurance product. In addition, most internet users are less aware of the cyber insurance coverage that helps cover losses resulting from cyberattacks. The rapid developments in technology and the increasing cyber risks that result from new techniques used by cybercriminals to execute cybercrimes have also led to the failure of the existing cyber insurance to meet the growing customer demands. Therefore, the study suggested a public-private partnership between the national security unit and insurance companies to establish policy measures that can address these challenges and support an effective cyber insurance market.

A study by Dalton et al. (2017) on building cybersecurity resilience in Africa noted that African countries cannot afford to be ignorant towards cybersecurity and must resist the misconception that cyber threats primarily affect developed countries. The study conducted a systematic literature review of studies on cyberattacks and cybersecurity measures employed in different African countries. According to the structural equation model analysis, the study identified that cyber resilience in African countries could be developed and sustained by implementing a cyber-resilience program (CRP) with effective responses to safeguard national cyber assets and citizens. Cybersecurity regulatory authorities should also develop and implement wide, coordinated, and all-encompassing approaches to address the vulnerabilities and risks that come with technological advancements. In addition, the study concluded that African countries should be more open and flexible to learn from other countries, looking outward to the international community and its local knowledge on how to prepare for, resist, and recover from cyberattacks.

Further, Akpan's (2020) study examined the extent of cybersecurity and cyber-resilience in Nigeria. The study adopted a descriptive research design, and the target respondents comprised IT experts, computer engineers, and security agents who have been exposed to computer science. The stratified random sampling technique was used to select the preferred sample from the total target population. A structured questionnaire was used to collect data from the selected sample. The findings from the data analysis revealed that the most commonly used strategy in Nigeria was putting in place a well-defined policy on Critical Information Infrastructure Protection (CIIP), while the least used strategy was developing partnerships between public and private organizations that can work together to establish an overall approach of security practices needed to protect critical infrastructure. As a result, the study recommended the establishment of an effective Computer Emergency Response Team at the national level, implementing a clear Critical Information Infrastructure Protection (CIIP) policy, and improving ICT infrastructure security and resilience.

A study by Waithaka (2016) assessed the factors affecting cybersecurity in national government ministries in Kenya. The study used a descriptive research design where the target population consisted of the ICT officers in ministries and internal auditors who are involved in the review of Information Systems. A structured questionnaire was then administered to the select respondents to obtain primary data for analysis. The findings of the study revealed that the key factors affecting cybersecurity are lack of management support in implementing and adhering to cybersecurity policies and requirements, employee system exploitation for personal gain, and system disruption and manipulation of system weaknesses. Thus, the study recommended that the management of Kenyan Ministries should put extra effort into understanding how cyberattacks affect the provision of services to its customers. Cybersecurity challenges need to be promoted even to the political elite to effectively influence government funding allocation on cybersecurity and encourage adherence to cybersecurity policies.

Ogonji (2019) also examined the nature of cyberterrorism in Kenya, the methods employed to counteract it, and the overall impact it has on national security. The study was guided by the deterrence theory and employed the exploratory research approach. According to the study's findings, Kenya has developed cyber security strategies and measures, including a legal framework, which is a crucial first step in establishing a dependable environment for people and businesses. However, cybercrimes have persisted with an increased risk and vulnerability of the technology users taken advantage of by cybercriminals. These strategies include a multi-agency approach, a legal framework developed under the Computer Misuse and Cybercrimes Act (2018), which outlines the legal policies and mechanisms to deal with cyberattacks, enhance technical capability through training and awareness campaigns, and promote cooperation with international partners. The study advocated a need for national security to engage other private sectors that can play an effective role in enhancing public participation and making better decisions on implementing surveillance and monitoring systems to improve cyber detection on online platforms.

Ouma (2021) analyzed the effectiveness of localized cyber incident response techniques and legal frameworks in Migori County, Kenya. The study used descriptive research approaches that targeted 121 Migori County staff members. The study then used Yamane's formula to obtain a sample size of 93 respondents from the target population. The findings of the study disclosed that the independent variables, such as policies, risk management, resources, and training, are positively correlated to effective cyber incident response techniques and legal frameworks. However, the low cyber incident response capability among county governments is often attributed to the fact that most county staff are unaware of the cyber risks since they assume that it is the responsibility of the management of information systems security to address cases of cyber threats or risks. In addition, the new cyber threats experienced due to the devolved ICT-enabled services, require localized cyber incident response techniques and legal frameworks since ICT management between counties varies. The study concluded by advising the county governments in Kenya to follow and administer the proposed localized framework for cyber event response.

Another study by Lukorito (2015) investigated Information security threats and E-government initiatives at the Kenya Revenue Authority (KRA). The study employed the descriptive research design and targeted the ICT officers in the KRA. The study also collected primary data through the use of structured questionnaires. The results of the study revealed that most of the participants outlined that KRA is still experiencing challenges in developing sustainable cybersecurity mechanisms and legal frameworks, particularly in the adoption of the online tax portal platform for better service delivery. The main challenges, as described by the study, were system disruption and manipulation of system weaknesses, business rivalry, system exploitation for illicit strategic planning insights, system attacks resulting from ideological conflicts, and employees' system exploitation for personal gain. As a result, the study recommends that policymakers in government ministries implement better policies that will address the ethical and political issues of employee involvement in the misuse and destruction of government systems for selfish gains.

While the studies mention the implementation of cybersecurity strategies, legal frameworks, and other measures, there is a gap in evaluating the effectiveness of these measures in countering cyber threats and terrorism. Future research should focus on assessing the impact and outcomes of implemented counter-terrorism measures and risk preparedness strategies in the telecommunication sector. Overall, more in-depth and empirical research is needed to fill these study gaps and provide a comprehensive understanding of counter-terrorism measures, risk preparedness, and cybersecurity in the telecommunication sector in Kenya.

5. Methodology

The research design refers to the overall structure and framework that guides the research process, including the selection of research methods and procedures, helps in achieving the main purpose of the study, and provides answers to the research (Aggarwal & Ranganathan, 2019). In this study, a descriptive research technique was employed to analyze

the different counter-terrorism measures on cyber threats and the level of risk preparedness in the telecommunication sector in Kenya.

The descriptive research design was chosen because it focused on providing a comprehensive description of the phenomenon of interest. It seeks to answer questions such as who, what, where, and how, aiming to accurately identify characteristics, frequencies, trends, and categories within the data (Nassaji, 2015), hence quantitative. By adopting a descriptive research design, the study aimed to minimize bias and maximize reliability in data collection and analysis.

This design allowed the researcher to collect data from a variety of sources, such as existing records, reports, and surveys, to gain a thorough understanding of the counter-terrorism measures and risk preparedness in the telecommunication sector in Kenya, a case study of Safaricom Head Office. The data collected was analyzed to identify and report the current state of affairs, providing a clear picture of the counter-terrorism measures implemented and the level of risk preparedness in the sector (Kreth & Bowen, 2017).

Overall, the descriptive research design enabled the study to fulfill its objective of providing a detailed description of the counter-terrorism measures in cybersecurity and risk preparedness in the telecommunication sector, shedding light on the characteristics, trends, and frequencies.

The objective was to examine the role of cybersecurity legal frameworks in shaping the risk preparedness of the telecommunication sector in Kenya. Results showed that the majority of the respondents, who were 66.66%, agreed that the company complies with the requirements of the Communications Authority of Kenya. It was also found that 71.43% of the respondents agreed that the company invests in educating its staff on IT infrastructure protection policies. Similarly, 80.95% of the respondents agreed that the company invests its financial resources in ensuring compliance with CA. The results further showed that the majority of the respondents (76.19%) agreed that the company invests in educating its staff on compliance with CA. On whether the company complies with the IT infrastructure protection policies, 71.43% agreed. In addition, 80.95% agreed that the company invests its financial resources in ensuring compliance with IT infrastructure protection policies.

The results from correlation analysis showed that there was a positive and significant relationship between cybersecurity awareness programs, data access control measures, cybersecurity legal frameworks, and the level of risk preparedness in the telecommunication sector in Kenya. Similarly, findings from regression analysis showed that cybersecurity awareness programs, data access control measures, and cybersecurity legal frameworks have a positive and significant effect on the level of risk preparedness in the telecommunication sector in Kenya.

6. Discussion

The third objective of the study was to examine the role of cybersecurity legal frameworks in shaping the risk preparedness of the telecommunication sector in Kenya with a focus on Safaricom's head office in Nairobi. From the findings, the company complies with the requirements of the Communications Authority of Kenya. It was also found that the company invests in educating its staff on IT infrastructure protection policies. The findings corroborate that of Gopal and Maweni (2019), who found that regulatory compliance in the telecommunications industry ensures network security and protects sensitive customer information. Since Telecommunication companies often handle large volumes of personal and confidential data, compliance with data protection and privacy regulations is paramount (Albers, 2022).

Similarly, it was found that Safaricom's head office invests its financial resources in ensuring compliance with CA. The results further showed that the company invests in educating its staff on compliance with CA and that the company complies with the IT infrastructure protection policies. The company also invests its financial resources in ensuring compliance with IT infrastructure protection policies. The results align with that of Ogonji (2019), who established that training programs play a vital role in enhancing employees' awareness of regulatory requirements and promoting compliance with IT infrastructure protection policies. Well-informed and educated staff members are more likely to understand and follow the established protocols, reducing the risk of security breaches and non-compliance.

The findings from correlation analysis show that there was a positive and significant relationship between cybersecurity legal frameworks and the level of risk preparedness in Safaricom's head office, Nairobi ($r=0.715$, $p=0.007$). This means that improving the cybersecurity legal frameworks leads to improved risk preparedness. Regression analysis further showed that cybersecurity legal frameworks have a positive and significant influence on the level of risk preparedness ($\beta=0.158$, $p=0.002$). This implies that a unit increase in data access control measures would lead to an increase in risk preparedness by 0.158 units. This agrees with the findings by Lukorito (2015), who found that institutions operating in countries with more robust cybersecurity regulations demonstrated higher levels of risk preparedness. According to Ouma (2021), legal frameworks provide organizations with a structured approach to cybersecurity, offering guidance on how to identify, assess, and manage risks effectively. In addition, legal frameworks often require organizations to implement specific cybersecurity measures and practices, such as risk assessments, incident reporting, and data breach notification protocols. Compliance with these requirements can enhance an organization's risk preparedness by ensuring that appropriate security controls are in place and that incidents are promptly identified and addressed immediately (Dalton et al., 2017).

7. Conclusion

The study aimed to understand the complex interaction between the changing regulatory landscape and Safaricom's cybersecurity risk mitigation techniques. The findings emphasize the need to adhere to legal frameworks in risk preparedness. Safaricom's adherence to the Communications Authority of Kenya's regulations, together with investments in training employees on IT infrastructure protection procedures, demonstrates the company's dedication to regulatory

compliance. This is consistent with the broader industry context, in which regulatory compliance is regarded as critical for protecting networks and sensitive consumer information.

Furthermore, the positive correlation and considerable influence shown between cybersecurity legislative frameworks and risk preparation highlight the beneficial effect of legal measures on an organization's ability to effectively manage and respond to cyber threats. The study demonstrates that strong legal frameworks give a disciplined approach to cybersecurity, assisting firms in discovering, assessing, and managing threats. Compliance with these standards not only requires the adoption of specific cybersecurity measures but also promotes a culture of early incident detection and mitigation.

According to (Musya et al., 2023), from the indigenous leadership perspective, cybersecurity plans can ideally be frequently prioritized through diversity and community involvement. This could lead to recommendations for Safaricom to implement more inclusive cybersecurity plans that consider the opinions and demands of many stakeholders, both inside the corporation and in the broader Kenyan community. As a result, this study serves as a foundation for continued research and development of comprehensive cybersecurity strategies in the telecommunications industry, considering the dynamic interplay between legislative frameworks, organizational practices, and the larger socio-cultural setting.

8. References

i. Aggarwal, R., & Ranganathan, P. (2019). Study designs Part 2–descriptive studies. *Perspectives in Clinical Research, 10*(1), 34.
ii. Albers, M. (2022). Surveillance and data protection rights: data retention and access to telecommunications data. In M. Albers (Ed.), *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches* (pp. 69–112). Cham: Springer International Publishing.
iii. Balzacq, T., & Guzzini, S. (2015). Introduction: 'What kind of theory - if any - is securitization?' *International Relations, 29,* 97–102. https://doi.org/10.1177/0047117814526606a
iv. Bechara, F. R., & Schuch, A. S. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime, 28*(2), 359–374.
v. Burton, J., & Lain, A. C. (2020). Desecuritising cybersecurity: Towards a societal approach. *Journal of Cyber Policy, 5*(3), 449–470.
vi. Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis.* Colorado: Lynne Reinner.
vii. Cariolle, J. (2021). International connectivity and the digital divide in Sub-Saharan Africa. *Information Economics and Policy, 55,* 100901.
viii. Elert, N., & Henrekson, A. M. (2021). Entrepreneurship prompts institutional change in developing economies. *The Review of Austrian Economics, 34,* 33–53.
ix. Guzzini, S. (2011). Securitization as a causal mechanism. *Security Dialogue, 42,* 4–5.
x. Imamov, M. A. (2021). The impact of the digital revolution on the global economy. *Linguistics and Culture Review, 5*(54), 968–987.
xi. José Zapata Campos, M., Barinaga, E., Kain, J.-H., Oloko, M., & Zapata, A. P. (2023). Organizing grassroots infrastructure: The (in)visible work of organizational (in)completeness. *Urban Studies, 60*(1), 126–145.
xii. Kreth, M. L., & Bowen, E. (2017). A descriptive survey of technical editors. *IEEE Transactions on Professional Communication, 60*(3), 238–255.
xiii. Makulilo, A. (2016). *African Data Privacy Laws.* Germany: Springer International.
xiv. Mitullah. (2022). Cybersecurity framework in Kenya. Mitullah Shako law. Retrieved from: https://mitullahshakolaw.com/the-cyber-security-framework-in-kenya/
xv. Musya, J. K., Bukusi, A. D., & Korir, A. J. (2023). How indigenous leadership research in Africa can inspire national prosperity. *Open Journal of Social Sciences, 11,* 134–155. https://doi.org/10.4236/jss.2023.117010
xvi. Muthuri, R., Capecchi, S., Sulis, E., Amantea, I. A., & Boella, A. G. (2022). Integrating value modeling and legal risk management: an IT case study. In R. Muthuri, S. Capecchi, E. Sulis, I. A. Amantea, & A. G. Boella (Eds.), *Information Systems and e-Business Management* (pp. 1–29).
xvii. Safitra, M. F., Lubis, M., & Fakhrurroja, A. H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369.
xviii. Stritzel, H. (2014). Securitization theory and the Copenhagen school. In *Security in Translation.* London: Palgrave Macmillan.
xix. UNCTAD. (2021). UNCTAD. Cybercrime legislation worldwide. Retrieved from: https://unctad.org/page/cybercrime-legislation-worldwide.