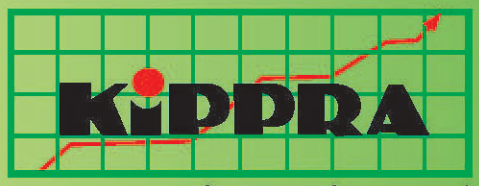
Discussion Paper Series



The KENYA INSTITUTE for PUBLIC POLICY RESEARCH and ANALYSIS

Cyber Security in the Wake of the Fourth Industrial Revolution in Kenya

Martin Kabaya and Mary Kageni

DP/326/2024

THE KENYA INSTITUTE FOR PUBLIC POLICY RESEARCH AND ANALYSIS (KIPPRA)

YOUNG PROFESSIONALS (YPs) TRAINING PROGRAMME

Cyber Security in the Wake of the Fourth Industrial Revolution in Kenya

Martin Kabaya and Mary Kageni

Kenya Institute for Public Policy Research and Analysis

KIPPRA Discussion Paper No. 326
2024

KIPPRA in Brief

The Kenya Institute for Public Policy Research and Analysis (KIPPRA) is an autonomous institute whose primary mission is to conduct public policy research leading to policy advice. KIPPRA's mission is to produce consistently high-quality analysis of key issues of public policy and to contribute to the achievement of national long-term development objectives by positively influencing the decision-making process. These goals are met through effective dissemination of recommendations resulting from analysis and by training policy analysts in the public sector. KIPPRA therefore produces a body of well-researched and documented information on public policy, and in the process assists in formulating long-term strategic perspectives. KIPPRA serves as a centralized source from which the Government and the private sector may obtain information and advice on public policy issues.

Published 2024

Bishops Garden Towers, Bishops Road
PO Box 56445-00200 Nairobi, Kenya
tel: +254 20 2719933/4; fax: +254 20 2719951
email: admin@kippra.or.ke
website: http://www.kippra.org

ISBN 978 9914 738 65 0

The Discussion Paper Series disseminates results and reflections from ongoing research activities of the Institute's programmes. The papers are internally refereed and are disseminated to inform and invoke debate on policy issues. Opinions expressed in the papers are entirely those of the authors and do not necessarily reflect the views of the Institute.

This paper is produced under the KIPPRA Young Professionals (YPs) programme. The programme targets young scholars from the public and private sector, who undertake an intensive one-year course on public policy research and analysis, and during which they write a research paper on a selected public policy issue, with supervision from senior researchers at the Institute.

KIPPRA acknowledges generous training on futures foresight methodology by EDHEC Business School, France; and the UNESCO Futures Literacy Laboratory Chair at Dedan Kimathi University of Technology (DeKUT), Kenya. The course on "Building Strategic Foresight Capabilities" by EDHEC Business School was beneficial for building capacity of Young Professionals on futures foresight.

Abstract

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Cybersecurity has been high on the agenda of the United Nations (UN) for a number of years. Kenya faces significant cybersecurity challenges due to rapid technological advancement. The integration of new technologies into critical sectors has increased the nation's vulnerability to cyber-attacks, data breaches, and other cyber threats. Despite the economic and social benefits brought by these technologies, the inadequacy of comprehensive cybersecurity policies and effective enforcement mechanisms leaves the country vulnerable against these evolving threats. The country in the recent past has experienced numerous cyber-attacks hence need for regular update of the cyber security policy and enforcement. This paper delved into the cyber security in the wake of the fourth industrial revolution. Cyber-attacks have been increasing over the years. It was evident that there is the inadequate trained personnels on cybersecurity and trained low operationalization of the ICT ward research centers. The study also establishes that increasing data breaches and cyberattacks have resulted in data losses, financial losses and denial of services. The study establishes technology advancement and regulatory framework as the main driving forces to the status of cyber security. Other factors found to significantly influence cyber security status are inadequate training on cybersecurity and insider threats. Thus, this calls for regular update and review of cybersecurity laws and policies to adapt to the evolving threat landscape and technological changes and that the laws align with global best practices and standards in addressing emerging cyber threats. There is need for adoption of high technologies in protection of devices against cyber-attacks. Cyber security awareness and training is very important and can be done through training institutions and the regular public campaigns to enlighten the public. Cyber security curriculum needs to be introduced in early learning to equips the future generation on matters cyber security

Abbreviations and Acronyms

ITU	International Telecommunication Union
M2M	Machine to machine communication
ICTA	Kenya Information and Communication Technology Authority
CAK	Communication Authority of Kenya
KICA	Kenya Information Communication Act
KE-CIRT/CC	National Kenya Computer Incident Response Team – Coordination Centre

Table of Contents

List of Tables

List of Figures

1. Introduction

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Cybersecurity has been high on the agenda of the United Nations (UN) for a number of years. The UN took up the subject out of recognition that building trust and confidence in the use of ICTs is crucial to the socio-economic well-being of humanity (International Telecommunication Union, 2024)). Cyber threat potential violation of security properties (ITU 2009). Cyber-attack occurs when a threat breaches security controls around a physical or an information asset. Threats and attacks are two important aspects from a security point of view. A threat is malicious act, that has the potential to damage the system or asset while an attack is an intentional act that causes damage to a system or asset. Cyber security also ensure that data, systems, and services are accessible and usable when needed and protected from disruptions, downtime, or denial of service attacks (Cinini, 2023).

Cyber security involves the process of preventing unauthorized access, alteration, disruption, or destruction of computer systems, networks, devices, and data. It includes a variety of tools, procedures, and methods intended to protect digital assets and guarantee the privacy, accuracy, and accessibility of data. Cyber security also ensures that data, systems, and services are accessible and usable when needed and protected from disruptions, downtime, or denial of service attacks (Cinini, 2023). The fourth industrial revolution (4iR) is the innovation age which involves innovative technologies such as mobile, social media, cloud, Internet of things (IoT), and Artificial intelligence (AI). With the applications of these technological systems, cybersecurity plays an important role in the rise of security in the field of Internet of Things, Blockchain and Artificial Intelligence.

The network that links different ICT (information, communication, and technology) infrastructure is known as cyberspace (Kang and Weskytte, 2018). The operation of commerce networks, emergency services, basic communications, national and international security systems, and other public and commercial operations all depend on cyberspace. In contrast to the actual spaces of land, sea, air, and space, cyberspace has grown to be a second place for human production and existence. It is currently the fifth largest strategic space.

However, the wide adoption and the evolving nature of cyberspace primarily driven by emerging technologies has created new risks (Cinini et al. 2023). These risks expose individuals, businesses, national infrastructure, and government to cyber threats emanating from a wide variety of sources both state and non-state and which manifest themselves in disruptive activities. Their effects carry significant risk to public safety, security of the nation and stability of the globally

linked economy. The Government of Kenya (GoK) continues to initiate and promote numerous cybersecurity policy and legal initiatives.

The Government has developed and enacted various policy, legal and regulatory frameworks that includes Data Protection Act 2019, National cyber security strategy 2022 and the Kenya Information and Communication act 1998 aimed at leveraging the opportunities of digital transformation to improve Kenya's economic development while ensuring digital safety of its people, businesses, and interests. Moreover, the Country's objective is to become a digitally empowered society and becoming an ICT hub for EAC. To achieve this the government has adopted e-government services and e-commerce. The Government has fully digitalized 5,084 government services and has gone a step further to identify a total of 9,362 government services to be digitalized (Communication Authority 2023).

As the government digitizes its operations, there is an increase in the attack surface from both inside and external actors in the digital space (Parn and Edwards, 2019). E-governance services involve the digitization storage of big amount of sensitive citizen data and information. Encryption, access, and secure storage measures need to be used to protect this data from unauthorized access and data breach. Similarly, the e-government platforms only accept online transactions for services payments such as Business licences and their renewals, tax payments hence need for robust measure to secure the e-government platforms to ensure integrity and confidentiality of the transactions and prevents fraud that leads to financial losses. 4IR is expected to revolutionize industrialization and accelerate economic development in the country to achieve the growth that is envisaged in the Vision 2030. However, the technological advancement and adoption in industrialization and in other government and private institution has brought about an increase in cybercrime rates (Świątkowska, 2020). The adoption of ICT systems in dispensing government services have necessitated Governments everywhere to pay close attention to Cybersecurity.

Cybersecurity is anchored on the following pillars: Cybersecurity governance, which is the framework, procedures, and organizational structures that businesses set up to efficiently manage and supervise their cybersecurity initiatives. It entails outlining the roles, duties, guidelines, and practices required to safeguard digital assets, reduce cyberthreats, and guarantee regulatory compliance. The second pillar is Critical information infrastructure protection, which describes the policies and procedures implemented to protect the vital networks and information systems that support a country's government, economy, and social structure. The third pillar is capacity building which involves training personnel on cybersecurity. It also anchored on Cyber risk and cybercrimes management, which involves monitoring and giving advisories in cyber threats. Further laws and Policy regulation pillar that are the set rules and policies on cybersecurity, and the las pillar is collaborations and cooperations between government and private companies as well as collaborations between nations on matters cyber security (Bruggemann, Koppatz, Scholl, and Schuktomow, 2022).

Cyberspace has a dynamic nature with perpetrators tactics that are evolving

constantly that expose the nation peace and stability. The Country still faces significant cybersecurity risks and challenges that can jeopardize both digital transformation agenda and national security. This is due to the heightened digital connectivity that has made the country more vulnerable to cybercrime. As the fourth industrial revolution takes phase, Cyber threats are expected to be more rampant due to adoption of more sophisticated technology by the perpetrators. It is under this backdrop that this paper looked at the cyber security status in the wake of 4IR.

There were approximately 339 million, 700 million and 860 million online crimes reported in in the Country for the years 2021,2022 and 2023 respectively. In 2023 between July and September Kenya registered over 123 million cyber threats, (Communication Authority,2023). The rise in cyber threats calls for a comprehensive examination of the current regulatory and policy framework. Analysis of historical trends in cyber-attacks and their evolving characteristics over the years is also crucial. Additionally, anticipating the future landscape of cyber threats, particularly in the context of the fourth industrial revolution, is essential for effective preparedness and response. This research aimed to i) Analyse the trends of cyber-attacks. ii) Assess the cyber security policy and regulatory framework. iii) Explore the future of the cyber security scenarios and proactive countermeasure in the wake of 4IR.

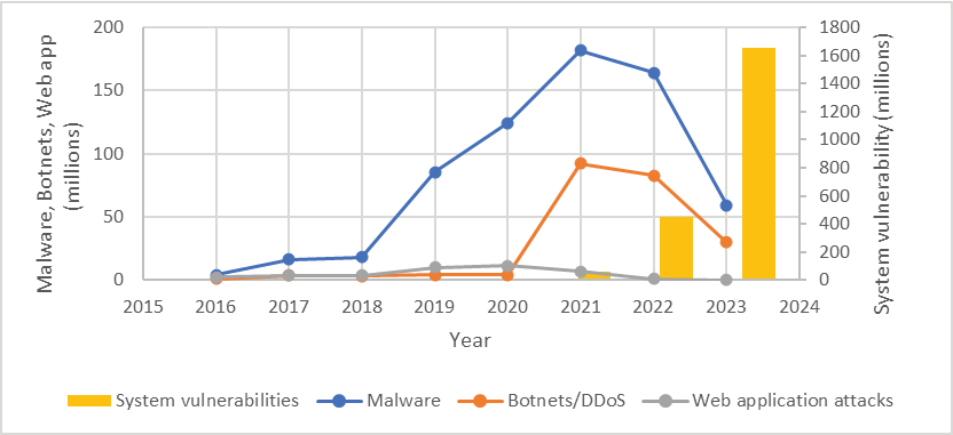
The organization of this paper is in six sections. paper has 6 sections. The first section is the introduction as discussed above. The second section covers the stylized facts on cybersecurity in the country. The third section discusses both theoretical and empirical literature on cyber security and the fourth industrial revolution. The fourth section discusses the methodology applied in the research., the fifth section is discussing the findings of the study, and the sixth section is the conclusion and policy recommendations.

2. State of Cyber Security in Kenya

2.1 Trends in Cyber Security

Trends in cyber security show that there has been increasing cybercrime incidences in the country in recent past. However, the government also through National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) has been able to identify and issues advisories on numerous types of cyber-attacks which is a measure of mitigating the number of cyber-attacks.

Figure 2.1: Trends in different types of cybersecurity in Kenya 2015 to 2023



Source: KNBS Annual report, 2023

Figure 1 shows the trend of the four main cyber-crimes in Kenya for the period 2016 to 2023. System vulnerability is observed to be rising rapidly from 2021. System vulnerability has been on the rise due to use of outdate software and use of weak passwords. This can be associated with the rapid adoption of technology in government services as well as in the private sector. According to KNBS 2023, the uptake of new digital economy among all industries has been on the rise and stood at 39.7 percent. Other crimes: malware, botnets, and web application attacks have been rising as observed but not rapidly.

Malware is a type of malicious software designed to harm or exploit computer systems. In the Country, malware threats are a significant concern due to the widespread use of digital technologies. Common types of malwares in are ransomware that encrypts data and demands payment in exchange for the decryption key. Trojan horses are malicious programs disguised as legitimate software. Adware displays unwanted advertisements on a user's device. This tracks user behavior and collect personal data, this very common on computers and shared networks.

DDoS (Distributed Denial of Service) overwhelms a targeted system with traffic from multiple sources, causing it to become unavailable. DDoS attacks are a

growing concern due to the increasing reliance on digital technologies. Common types of DDoS this includes Network DDoS that have been targeting financial institutions and government agencies. Application DDoS have caused disruption on critical services such as online banking and e-commerce platforms.

Web Application Threat involves exploiting vulnerabilities in web applications to gain unauthorized access or disrupt services. SQL injects malicious code into a web application's database to extract or modify sensitive data. Another type is the cross-Site Scripting (XSS) that is a malicious code used by attackers to steal data or take control of the user's session. This is particularly targeting social media and online banking platforms.

System vulnerability threats involve exploiting weaknesses in operating systems, software, or hardware to gain unauthorized access or disrupt services. In Kenya, system vulnerability threats are of significant concern due to the widespread use of outdated or unpatched systems. The unpatched system attacks have occurred in government agencies and financial institutions. Moreover, the use of weak passwords or easy to guess password make systems vulnerable to unauthorized access and this is common among the individuals and small businesses.

Kenya has experienced a rapid growth in the number of cyber-attacks carried out in the past 5 years. The communication authority in the same period has been giving out advisories to different government and private institutions on attacks. The advisories have been increasing with time. However, the number of advisories issued, and the number of attacks experienced has a big difference explaining a possible reason for the high number of cyber-attacks executed. Graph 2 shows the total number of cyber-attacks and advisories issued in Kenya for the period 2017 – 2023.

2.2 Technological adoption in Kenya

The country has experienced an exponential adoption of the M2M communication and mobile transactions that is facilitated by technological advancements and the widespread adoption of IoT devices. M2M communication boost efficiency in operational and data sharing across industries, supporting automation and smart infrastructure (Fig 2). Moreover, the smartphones and mobile internet has fueled the growth of mobile transactions, offering convenient and accessible financial services that has led to inclusion of the unbanked population (Fig. 3). These innovations ensure seamless connectivity and financial inclusion thus transforming how businesses operate, and individuals manage finances as illustrated in the figure 2 and figure 3 below.

Figure 2.2: Machine to Machine communication

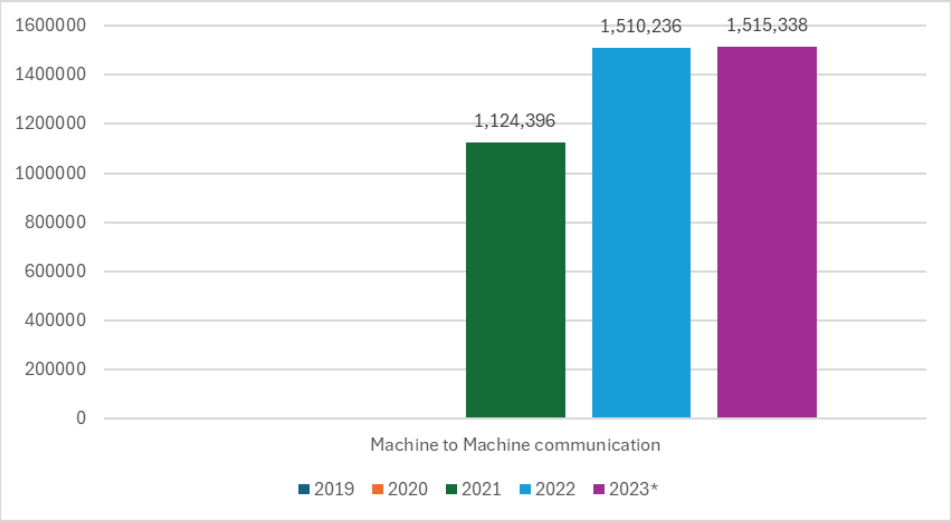
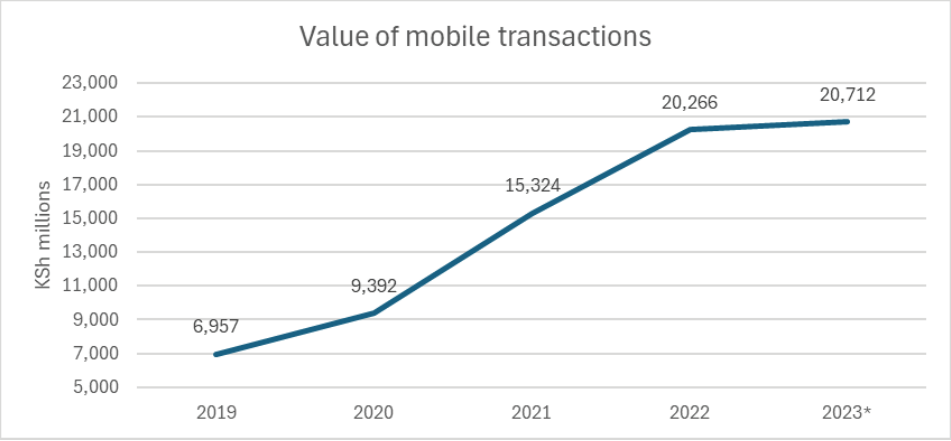


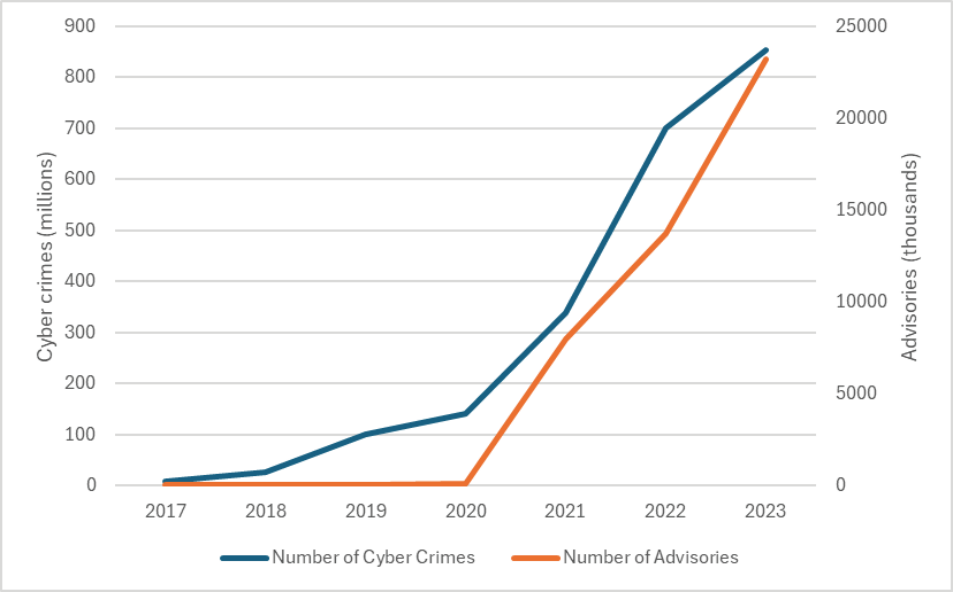
Figure 2.3: Mobile transactions



Source: Kenya National Bureau of Statistics (2024)

Cybersecurity in M2M communication and mobile banking is very critical, as these systems are vulnerable to cyberattacks. Cyber security involves use of robust encryption, authentication protocols, and intrusion detection systems to protect data integrity, confidentiality, and availability. As M2M and the mobile transactions grow, advanced security measures key to safeguard against evolving threats and ensure reliable and secure communication between machines and online transactions.

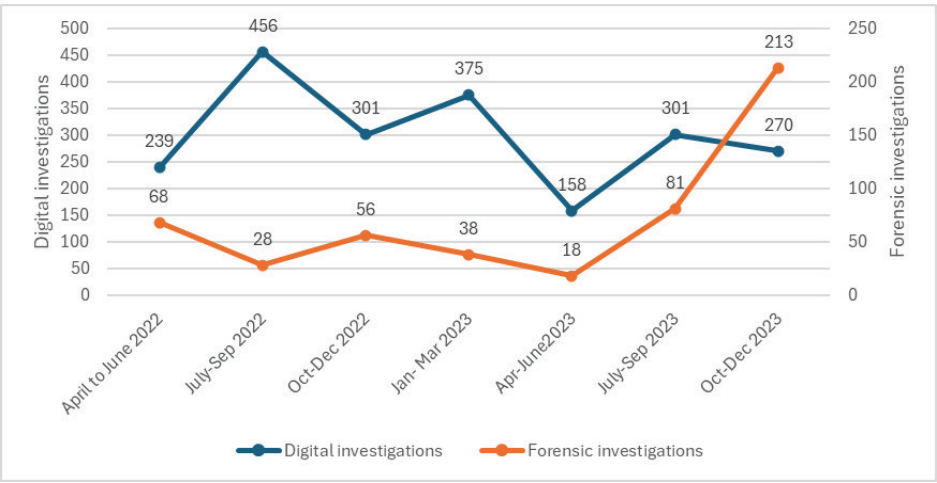
Figure 2.4: Number of cybercrimes and advisories in Kenya for 2017 to 2023



Source: Communication Authority of Kenya (2024)

Digital investigations and forensic investigations on cybercrimes have been reported and conducted over time in the country. Figure 3 shows the dynamic of both digital and forensic request by Kenyans from April 2022 to December 2023. There has been a growing number of cyber crime and the advisories of the same.

Figure 2.5: Digital and Forensic investigations Requests April 2022 – December 2023



Source: Communication Authority of Kenya, 2024

Figure 5 shows that there has been a varying trend in the number of digital investigations made in the country. The same can be used for the forensic investigations requests but from April 2023 there was an upward trend in the number of forensic requests made in the country due to cyber threats.

3. Policy, Legal and Institutional Framework

3.1 Policy Framework relating to Cyber security

Kenya has been actively committed to strengthen cyber security through development and implementation of regulatory frameworks these includes:

Emerging technology and the cyber security policy

Internet of Things (IoT) technology is one of the emerging technologies that the regulatory framework seeks to address. The National Cybersecurity Strategy, 2014aims to build a secure and resilient cyberspace that is key for the growth of IoT applications. Kenya Information and Communications Act, 1998 (KICA) outlines the functions of the Communication Authority (CA) in electronic transactions and for IoT deployments, e-transaction is also an emerging technology. Moreover, the Communication Authority and institution developed through KICA has developed guidelines on the use of IoT devices and outlines the procedures for IoT deployment in Kenya. Further, the CA provides guideline to ensure that that all citizens have access to at least 3G connectivity, which is essential for the widespread adoption of IoT technologies.

National broadband strategy, 2018 seeks to promote the country's digital infrastructure and promote the adoption of broadband services by ensuring 5G connectivity, fiber optic network connections and the satellite broadband connections in the remote areas. Moreover, the Data Protection Act (DPA), 2019 advocates for the protection of personal data, including data collected through IoT devices. The policy further requires the IoT service providers to implement technical and organizational measures to ensure privacy. Computer Misuse and Cybercrimes Act (CMCA),2018, criminalizes cyber-related offenses, including those that involve IoT devices, such as unauthorized access, system interference, and cyberbullying.

Artificial intelligent is another emerging technology that has been factored in the Kenya's Digital Economy Blueprint, 2019 that advocates for development of digital skills framework in AI. Kenya's National ICT Policy, 2019 advocates for consideration of the trends in big data, machine learning, and AI as emerging technologies that the country needs to be keen on. Further, Kenya National Digital Master Plan 2022-2032 calls for the development of a National AI Strategic Plan. Kenya Bureau of Standards (KEBS) has developed a draft code of practice that provides guidelines on development and use of AI systems. The media industry has guidelines provided by the Media council of Kenya that has provisions on the use of AI in industry and handbook for reporting on AI. Robotics a technology that is widely being used in Kenya for instance in in 2023, UNDP Kenya and the Ministry of Health launched a pilot of smart anti-epidemic robots, funded by Japan, at Kenyatta National Hospital and Jomo Kenyatta International Airport to combat COVID-19. Kenya's National ICT Policy highlights the importance of robotics.

Cyber security training and awareness

The government has identified cyber skilling as one of the key initiative by ensuring trained workforce as envisaged in National Cybersecurity Strategy (2022-2027).The Communications Authority of Kenya (CA) also conducts regular campaigns and awareness to cybersecurity through training programs for various stakeholders that includes the government agencies, private sector organizations, and the general public. Similarly, the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) organizes capacity building workshops and training sessions for stakeholders to sharpen their skills on threats detect, prevent, and respond to cyber threats as envisaged in National Digital Master Plan, 2022.

Moreover, the government collaborates with the in regional and global cybersecurity capacity building initiatives, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the International Telecommunication Union's (ITU) Global Cybersecurity Index. Further, the establishment of National Cybersecurity Centre a hub for cybersecurity research, training, and innovation. National Commission for Science, Technology and Innovation, National Research Fund and Kenya National Innovation Agency Science, Technology, and Innovation Act, 2013 KENIA was developed to manage the National Innovation System within the country and take part in cyber security research and development.

Cyber security governance

Comprehensive cyber security framework has been developed to combat cyber threats and vulnerabilities. In terms of governance the National Cybersecurity Strategy (2022) was developed to strengthen legal frameworks, protect critical information infrastructure, and build cybersecurity capacity. The Computer Misuse and Cybercrimes Act (2018) seeks to address the offenses such as unauthorized access, cyber espionage, harassment, and terrorism, through effective detection, prevention, and prosecution of cybercrimes. Further, Kenya Information and Communications Act (1998) gives Communications Authority of Kenya mandates to develop national cybersecurity management guidelines. Similarly, data privacy and protection are handled by the Data Protection Act (2019) that safeguards personal data, mandating protections against unlawful data handling.

Additionally, the Central Bank of Kenya's provides the procedure to be followed on Payment Service Providers to ensure a secure cyberspace within the financial sector. The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) that is multi-agency body coordinate cybersecurity responses and manage threats continuously. The team is made up of the Law Enforcement Agencies that includes the National Computer and Cybercrimes Coordination Committee, judiciary, National police and the Kenya defense forces to ensure that the offenders are identified, investigated, and brought to justice. Similarly, the Kenya Robotics and Artificial Intelligence Society Bill 2023 proposes fines unlicensed robots' operators and AI. The proposed sanctions include up to

KES 1 million ($6,250) and/or two years' imprisonment for unlicensed entities operating in robotics and AI if they fail to register with the Robotics Society of Kenya (RSK), which will oversee the sector's growth through regulations.

3.2 Institutional Frameworks in Kenya Mandated to Handle Cyber Security

The Ministry of ICT was developed to develop, implement the national ICT, and cyber security policies and strategies.

Kenya ICT Authority (ICTA) a state corporation under the State Department of ICT was developed through a Legal Notice No. 183 of August 2013. ICTA was seen as the vehicle for executing and operating all information systems services and ICT infrastructure projects in the public sector.

The Communication Authority of Kenya (CAK) was created in 1999 under the Kenya Communication Act of 1998 (KICA 1998), it has overseen the phenomenal growth of the telecommunications, broadcasting, internet and mobile money transfer services in Kenya.

The National Communication Secretariat (NCS) which is under the State Department of ICT is responsible for policy development that was established through the Kenya Communications Act of 1998 that continue to be the policy advisory arm of the Government on all matters pertaining to the ICT sector.

National Computer and cybercrime coordination committee that coordinates the cyber security initiatives within the country. The committee is composed of various government agencies that includes the Criminal Investigation Directorate, National Police. Office Of the Data Protection Commissioner was established to oversight and enforce the personal data and information protection by all agencies. Konza Technopolis Development Authority (Kotda) and university are mandated to offer Research and training in cyber security.

Policy gaps

Kenya has development policies to address cyber security. However, inadequate skilled personnel in Cyber security and low operationalization of the ICT ward research centers remain their short coming. Moreover, inadequate resources to implement cyber security policies and programs and evolving technological advancement are also posing a serious limitation to cyber security.

Fragmented reporting systems of the cyber security whereby you find if an incident occurs most of the time there is no clear guideline on who is responsible for example DDOS attack on the e-government services most of the agencies did not have a clear answer on who was responsible. Moreover, there is legal ambiguity, cybercrime keeps on changing every day whereas the laws does not evolve at the same speed. Hence difficult to prosecute cybercrimes effectively and a clear guidance on reporting obligations.

4. Literature Review

This section presents similar studies that has been done on cyber security. The section has the theoretical framework and the empirical literature.

4.1 Theoretical Literature

4.1.1 Diffusion of Innovation Theory

This theory was fronted by Everett Rogers in 2003, explains how new concepts, methods, or tools are gradually embraced by people and communities. Both the organizational and personal levels can benefit from the application of the Diffusion of Innovations Theory (DOI). It illustrates the how, why, and rate at which novel concepts spread across cultural boundaries. The DOI hypothesis, according to Rogers (2003), views innovation as something that happens over a considerable period and is disseminated through specific channels. According to Rogers (2003), people typically take a long time to accept new technology. Relative advantage, compatibility, observability, trialability, and complexity are important criteria that affect adoption. People are said to have varying degrees of interest in accepting innovation, and that this varies per individuals. This theory forms the basis for studies on information and technology adoption and diffusion.

4.1.2 Technology organization environment framework

This framework was developed by Tornatzky and Fleischer in 1990. It identifies three dimensions of an organization's context that influence the diffusion and adoption process of innovations. This theory offers a comprehensive framework for comprehending the dynamics of technology adoption inside businesses. This theory states that variables related to the technology itself, the adopting organization, and the broader external environment all have an impact on the process of adopting new technologies. Consequently, when making decisions, decision-makers had to take organizational, technological, and environmental aspects into account.

4.2 Empirical Literature

Li, Y., and Liu, Q. (2021) carried out a study on the emerging trends of cyber security and found out that most of the economic, commercial, cultural, social, and governmental activities and interactions of countries, at all levels are done in the cyberspace. The study also found out that private companies and government organizations around the world are facing the problem of cyber-attacks. The study further found out that organizations today are highly dependent on electronic technology, and data protection from cyber-attacks is becoming major challenging issue. Cyber-attacks target to impact companies financially and some attacks were of political nature too. Moreover, the study identified types of cyber-attacks to include PC viruses, knowledge breaks, data distribution service (DDS) and other

assault vectors. Various organizations use several methods to curb damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data.

Mwangi, et. Al, 2022 study on cyber threats in Africa found out that there is an increased mobile phone and internet penetration in the African continent that brings a huge population of internet users in Africa that are vulnerable to cyber threats such as misinformation campaigns and cybercrime. Further, the geopolitical conflicts are changing to cyber security for example the Russian-Ukraine war and the US- China warfare. Moreover, in the Africa continent emergence of online election interference, has had major implications on peace, security, and development.

Pivoto et., al, 2021 found out that internet of Things (IoT) devices is rapidly becoming universal. The number of businesses entering the Industrial Internet is dynamically growing, by connecting industrial units through the internet to improve productivity and efficiency. Internet-enabled industries are key targets of Cyber Security threats, and it is one of the key challenges that need to be dealt with. Cyber security vulnerabilities target critical infrastructure and affects the entire business process and companies' reputations. Further, the hyper-connectivity between smart devices and smart networks offers an opportunity to cybercriminals who can easily identify weaknesses, insecure entry points in networks and sometimes the devices too.

Cyber-attacks not only cause an interruption to the standard functionality of an organization but also impact the overall society. The success of IoT can't be ignored in today's scenario; along with its attacks and threats on IoT devices and facilities are also increasing day by day. Cyber-attacks are becoming a part of IoT and affecting the life and society of users, so steps must be taken to defend cyber seriously. Cybercrimes threaten the infrastructure of governments and businesses globally and can damage the users in innumerable ways. MSP Managed Service Providers face Various difficulties in fighting with Cybercrime in this era of internet of things. The service providers need to ensure that customer's security as well as their security in terms of their servers, devices, and systems.

D'Adamo et al., 2021 study found out that e-commerce business entities and customers are always on the targets of cybercriminals and cyber-attacks. Attackers usually attack customers' private data that is the most asset in e-commerce. The cyber criminals acquire data from the database of online stores, malware, ransomware, and e-skimming. Further, they through distributed denial of services (DDoS) or Phishing. With the coming up of e-business and e-commerce opportunities are reaching customers very fast but not in the absence of issues like cyber security. Similarly, Jang-Jaccard and Nepal, 2014 found out that e-commerce organizations cybercriminals are also constant advancing their technology and skills to find vulnerabilities in the existing system of e-commerce and take advantage of them.

Taddeo and Floridi, (2019) in a study on trusting artificial intelligence found that Artificial intelligence (AI) is one of the key technologies of the Fourth Industrial Revolution that can be used for the protection of Internet-connected systems from

cyber threats, attacks, damage, or unauthorized access. The utilization of artificial intelligence (AI) for cybersecurity has been of great concern for private and the public sectors. The study indicated that the market for AI in cybersecurity has grown from US$1 billion in 2016 to a US$34.8 billion net worth by 2025. Further, they found out that latest national cybersecurity and defence strategies of several governments explicitly mention AI capabilities. However, use in cybersecurity tasks is a double-edged sword: it can improve cybersecurity practices, but also facilitates new forms of attacks to the AI applications which pose severe security threats Ghelani, (2022). Emerging technologies, technological advancement and change in regulations on cyber security play a significant role in shaping the status of cybersecurity. Chitech et al. (2021) Jang-Jaccard and Nepal (2014), Cinini et al. (2023); Hasani et al. (2023) all agreed that for cyberspace to be safe, technology and legal and regulatory framework must be prevailed.

The reviewed studies have shown how the emergence of technologies such as artificial intelligence, the Internet of Things, and blockchain has transformed various sectors, drove economic growth and enhancing service delivery. However, this technological brings about vulnerabilities, exposing critical infrastructures and personal data to sophisticated cyber-attacks. The studies have emphasized on the critical role of a robust legal and regulatory framework in mitigating these risks, noting that current cybersecurity laws in Kenya are often inadequate and lag technological developments. There is a consensus on the need for comprehensive legislation, effective enforcement mechanisms to bolster national cybersecurity resilience and ensure sustainable development in the digital age.

5. Methodology

The first objective of this study was achieved by a systematic policy review method in which a review of existing policies and regulations on cyber security was done. For the second and third objectives, this study adopted a DEFT Futures foresight approach. The foresight method has three categories which include quantitative, qualitative and semiquantitative. the semiquantitative method uses mathematical principles such as cross – impact analysis in order to quantify subjectivity, judgements and views that are sought from experts (Popper, 2008). This approach is used in assessing the drivers, enablers, frictions, and turners of cyber security (Gordon, 2010). It provides a basis for understanding the forces behind a trend, the factors that support these forces, factors resisting the trend as well as the factors that block the cyber security trend in Kenya in the wake of the fourth industrial revolution. DEFT has the following components, Drivers: forces that cause a trend to move and sustain it; Enablers: Factors that promote facilitate and catalyze a driver; Friction: resistance that impedes a trend; and Turners: forces that intend to oppose the trend.

It is possible to comprehend what the future looks like by putting into consideration the changes that have been brought about by the interaction between the drivers, enablers, frictions, and turners in the cyber security. The study makes assumptions based on the SWOT analysis on cyber security in the country. Drivers, enablers, turners, and frictions of cybersecurity were identified from literature and the first round of DELPHI questionnaire administered to identified respondents. 40 Key stakeholders were engaged in the first stage and the purpose of this engagement was to seek input on identified drivers, enablers frictions and turners and how they influence the status of cyber security. Thirteen indicators were identified from the 32 respondents and were used to prepare questionnaire for the second round DELPHI techniques. From the second round, 32 responses were received from a sample of 40 respondents. The responses were extracted, and correlation analysis was used to transform the data.

Micmac was later used to find out the levels of influence and dependence of each variable against each other. Pillkahn, (2008) argues that if a forecast is agreed upon by majority of experts, then it has greater credibility compared to that with opinions of an individual. The Micmac results were then used to build scenarios for the future of cyber security in the wake of 4IR.

Table 5.1: Analytical framework for; DEFT Analysis for Cyber Security in Kenya

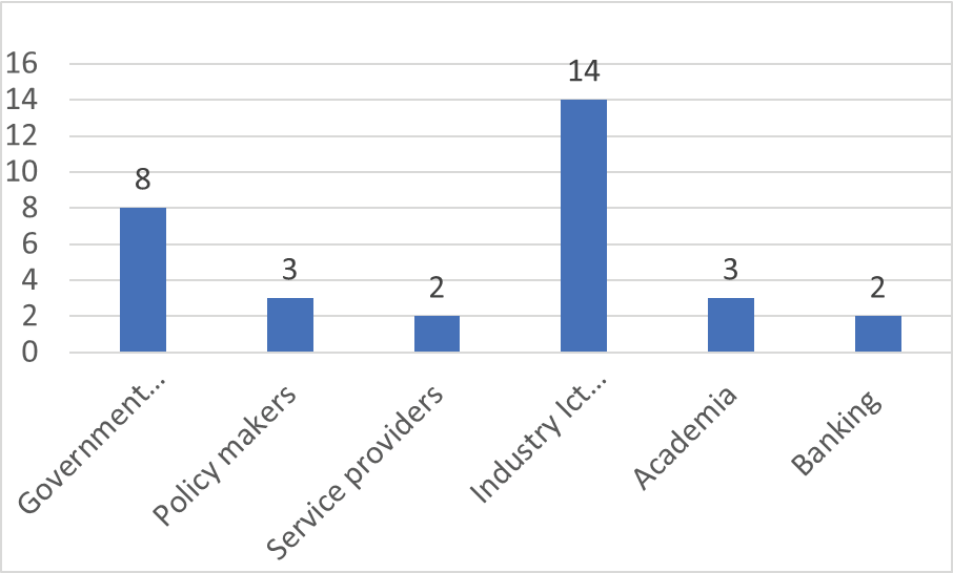
Cyber Security	Variable	Indicator
Drivers	Technology Advancement	Number of connected devices Number of E-commerce services Number of E-government Services
	Threats Landscape	Type of cyber-attack and the numbers
	Data Privacy Concerns	Number of data breaches
	Rate of technology adoption	Percentage of adoption
	Regulatory change	No. of new laws and regulations
Enablers	Artificial Intelligence and Machine Learning	Counts of projects within organizations and industries utilizing AI and ML
	Data Encryptions	Number of sensitive data encrypted and the level of awareness on data encrypted
	Policies and regulations	Effectiveness of existing laws and regulations
	Training on cyber security	Number of training forums and campaigns on cyber security
	Cyber threat advisories	
	Number of cyber-attacks warnings	Digital investigations Number of digital investigations conducted
	Digital forensics	Number of digital forensics carried out
Friction	Integration of security technologies	Number of unified security landscape Rate of technology adoption
	Dynamic nature of technology	Insider threats Number of insiders attacks
Turners	User behaviour change	Nature of change in use of technology

	Emerging technologies	Types of the upcoming technologies

5.1 Distribution of the respondents.

The number of respondents was 32 who were from different sectors. Figure 5 shows the distribution of these respondents per sector.

Figure 5.1. Respondents per sector



6. Discussion of Findings

Kenya has experienced an increase in cyber security breaches as shown by increase in cyber-attacks. This has resulted in financial and the data losses to the cyber criminals. Cyber criminals are upskilling their skills everyday due to increased use of social media that provide the criminals with easy learning platforms hence being ahead of the investigations and the forensic professional personnels.

6.1 Drivers of cybersecurity

From the literature, 15 variables were identified to have influence on the status of cyber security.

Table 6.1: Drivers of cyber security identify through literature review

Aspect	Driver	Sources
Driver	Technology Advancement	Jang-Jaccard, J., and Nepal, S. (2014), Cole et al. (2008) Neetesh (2020). Chitech et al. (2021)
	Threats Landscape	Li and Liu, (2021); Ghelani, D. (2022).; Neetesh (2020).
	Data Privacy Concerns	Casey (2011); Ngare, B. M. (2018).
	Rate of technology adoption	Mugarura, and Ssali, (2021); Hasani et al. (2023); Cole et al. (2008); Rotich, (2020)
	Regulatory change	Chitech et al. (2021); Fielder, J. D. (2021).; Sales, N. A. (2012).
Enablers	Artificial Intelligence and Machine Learning	Taddeo and Floridi, (2019); Pivoto et., al, 2021.; Ghelani, D. (2022).
	Data Encryptions	Casey (2011)

	Policies and regulations	Ghelani, D. (2022).; Sales, N. A. (2012).; Ngare, B. M. (2018).; Samoei, P. C., and Gatobu, P. (2024).; Mugarura, N., and Ssali, E. (2021).
	Training on cyber security	Mugarura, N., and Ssali, E. (2021).; Kaibiru et al. (2023); Chizanga et al (2022)
	Cyber threat advisories	Muhati, (2018)
Frictions	Integration of security technologies	Samoei, Pand Gatobu, P. (2024).; Jang-Jaccard, J., and Nepal, S. (2014).
	Dynamic nature of technology	Zhan et al. (2024).; Cole et al (2008).; Rotich, E. K. (2020).
	Insider threats	Li and Liu, (2021).; Ghelani, D. (2022).
Turners	User behaviour change	Ghelani, D. (2022).; Muhati, E. (2018)
	Emerging technologies	Cinini., Ehiane., Osaye., Irewunmi., (2023).; Chitechi (2021).; Ghelani, D. (2022).; Hasani et al. (2023)

6.2 Scenarios in Cyber security in Kenya

This study explains the possible future scenarios that may arise in cyber security due to fourth industrial revolution. Cyber security is ensuring that the systems that are used by different institution do not face attacks that are cyber related. This study identifies several types of cyber-attacks that have been carried out done by attackers. Also there have been numerous measures like advisories, trainings and forensic investigations that have been done to enhance cyber security. Through analysis of the trends of different types of cyber-attacks and different measures to curb the attacks, this study comes up with plausible scenarios in the cyber security in the country. The study made the following assumption based on the SWOT analysis conducted on the cyber security in Kenya.

Table 6.2: Assumptions based on SWOT Analysis of Cyber Security in Kenya.

SWOT	Assumption
Strength	• Fully implementation of the computer misuse act and cybercrime Act 2018 (CMCA)
	• Enhanced local and international collaborations on management of cybersecurity.
	• Enhanced capacity building on cyber security
	• Development of a new national security strategy on cybersecurity
	• A robust and well positioned National KE-CIRT/CC Kenya Computer Incident Response Team – Coordination Centre
Weaknesses	• Slow adoption of cyber security measures in both private and government institutions
	• Inadequate budgetary allocation on cybersecurity in both government and private institutions
	• Low cybersecurity training and capacity building
Opportunities	• Collaborations on cybercrime awareness and capacity building between public and private sectors
	• Government support towards an enabling cyber security effort by providing an enabling policy and legal framework
Threats	• Increase in use of more sophisticated technology by cyber threats perpetrators.
	• Rise in coordinated cybercrime groups

6.3 Cross Impact Analysis

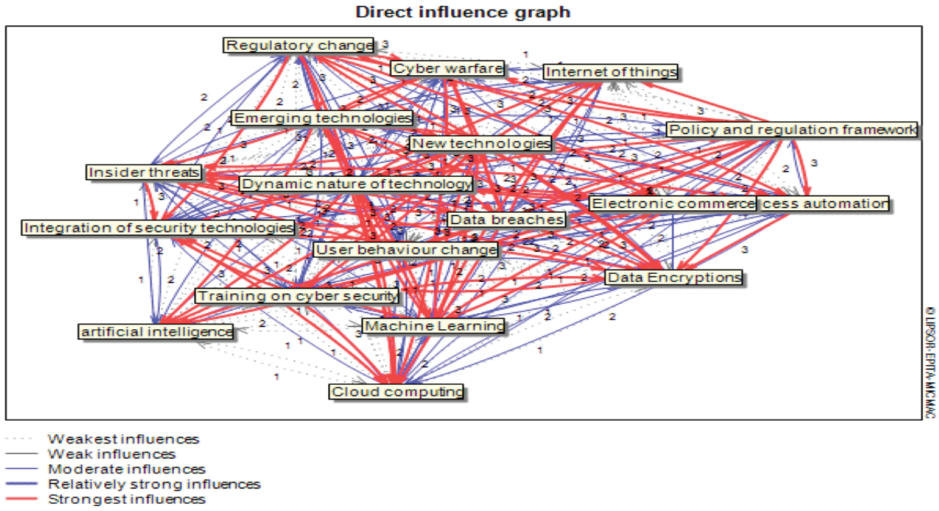
A cross-impact analysis matrix is an instrument for assessing how several variables or factors affect one another within a system. It entails building a table with rows and columns for different variables or factors, with each cell showing how one variable affects another (Culka and Society 2018). Cross impact emphasizes on potential consequences and interactions between components, and therefore aids in scenario planning and strategic decision-making, by helping to visualize dependencies and interconnections. From the matrix, level of interactions is indicated by numbers 0 to 3. zero (0) means that there is no influence between the

factors, 1 means low influence, 2 means there is a moderate influence between the factors while 3 means that there is a high influence between the factors. Table 3 below shows the matrix on how the DEFT variables affected and influenced each other.

Table 6.3: Cross-Impact matrix

	Process Automation	Data breach	Policy regulation	Insider Threats	Cloud computing	New technologies	Cyber Warfare	AI	Machine Learning	Data Encryption	Training	Ecommerce	IoT	Integration of Technology	Nature of technology	User behavior	Regulation Change	Emerging technologies
1: Process Automation	0	0	2	0	2	2	0	1	2	0	1	1	1	2	0	2	2	1
2: Data breach	3	0	3	3	3	3	3	3	2	1	0	2	3	3	1	3	1	1
3: Policy regulation	3	2	0	1	2	2	3	3	3	3	3	2	3	2	2	3	3	1
4: Insider Threats	3	3	1	0	2	1	2	2	3	3	3	3	3	3	2	3	2	1
5: Cloud computing	2	0	2	1	0	2	2	1	2	1	1	1	1	0	1	1	1	1
6.New technologies	2	1	2	1	2	0	3	3	3	3	3	3	1	0	3	1	3	2
7: Cyber Warfare	1	0	1	3	3	0	0	1	0	0	1	1	1	1	2	1	1	1
8: AI	1	0	1	0	1	1	1	0	1	0	1	2	0	1	2	0	1	2
9: Machine Learning	2	1	1	1	2	3	2	1	0	2	2	3	3	3	3	1	1	0
10.Data Encryption	0	1	1	0	1	1	2	0	2	0	3	2	1	1	2	1	2	1
11: Training	2	0	2	2	3	1	2	1	2	3	0	3	3	3	2	1	0	1
12: Ecommerce	0	1	2	0	1	1	1	1	1	0	0	0	1	1	3	2	1	0
13: IoT	1	2	0	1	2	1	2	0	1	1	2	1	0	1	1	1	1	1
14: Integration of Technology	2	1	0	1	3	2	1	2	1	3	1	2	2	0	2	2	2	1
15: Nature of technology	0	2	0	3	3	3	2	3	3	3	1	3	3	2	0	2	2	1
16: User behavior	1	1	0	3	2	1	1	0	1	2	1	1	0	1	1	0	2	1
17: Regulation Change	3	1	1	2	3	1	3	1	1	3	1	3	0	3	2	2	0	3
18: Emerging technologies	3	3	2	1	1	3	3	3	3	3	2	1	1	2	3	1	2	0

Figure 6.1: Variable Direct influence map



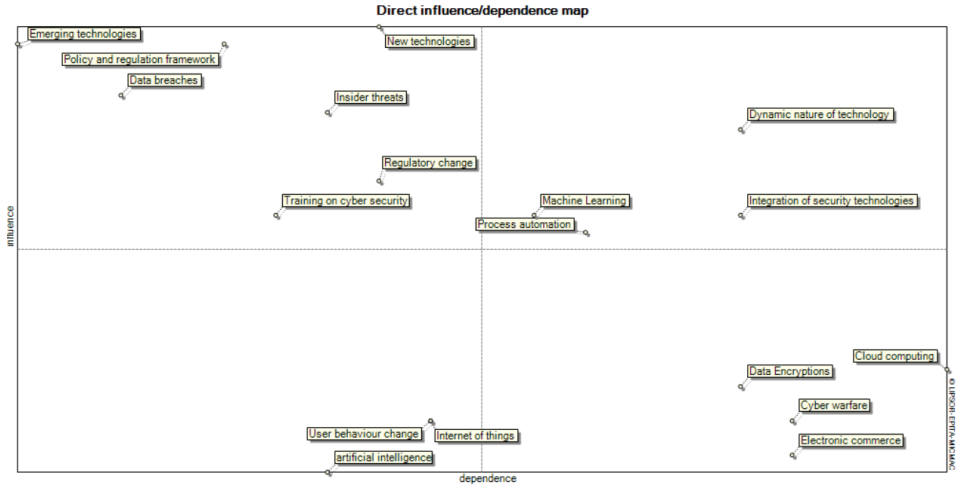
The MICMAC software maps the direct influence of each variable to the other. The direct influence graph shows the extent to which each variable under the study directly influences each other. The scale of influence is in 5 levels; weakest, weak, moderate, relatively strong, and strongest (Arcade et al. 1999). The variable with more red arrows pointing at it has more direct influence on the other variables.

Cross impact analysis creates a four-quadrant quartet map and represents four different variable types. Classification and distribution of these variable in the quadrant is determined by the levels of influence and dependence of each variable both representing the input and outputs respectively. The degree of dependency is represented by the horizontal axis while the level of influence is shown by the vertical axis (Alipour et al.2017).

The direct influence graph shows how each variable under the study directly influences each other. The variable with more red arrows pointing at it has more direct influence on the other variables.

The direct influence graph shows how each variable under the study directly influences each other. The variable with more red arrows pointing at it has more direct influence on the other variables.

Figure 6.2: Direct Influence- Dependency



The direct influence -Independence map shows the levels of direct influence and the level of dependence an indicator has on the dependent variable. The first segment on the top left show's indicators with the highest level of influence and lowest dependence level these factors are referred to as driving forces. These factors are controlled by the system behavior but have the highest influence on the system behavior. These factors are the most important because they are the driving forces of the system (Alipour et al.2017). The upper right segment shows the indicators with the high level of influence and high-level dependence. These factors are called the relay factors. The relay factors are highly dependent on other factor which makes them unstable and come bring about emergent outcomes in cybersecurity. The third segment represent the variables with high dependence level but low level of influence. They are referred to as the result factors. The last segment on the lower left represent variable with low influence and low dependence on cyber security. These are also referred to as autonomous factors. The summary of variable distribution to the four segment is shown in table 4.

From figure 6, New technologies is a very influential driving factor in the future of cybersecurity. Policy and regulation framework similarly is a driving force that is vital in reshaping cyber security. Emerging technologies is another factor that drives and shapes the future of cyber security. The number of emerging technologies will affect the status of cyber security in future (Zhan et al. 2014). The research also shows that data breaches and insider threats as important driving forces in shaping cybersecurity. The prevalence of data breaches and insider threats in different institutions, both public and private, will influence the status of cyber security in the future. Regulatory change is another factor that was found to be a driving force in cybersecurity status. Among the identified driving forces, training on cyber security was found to be weakest factor due to is position on the quadrant while new technology, policy regulations were the factors with highest impact on the status of cybersecurity respectively.

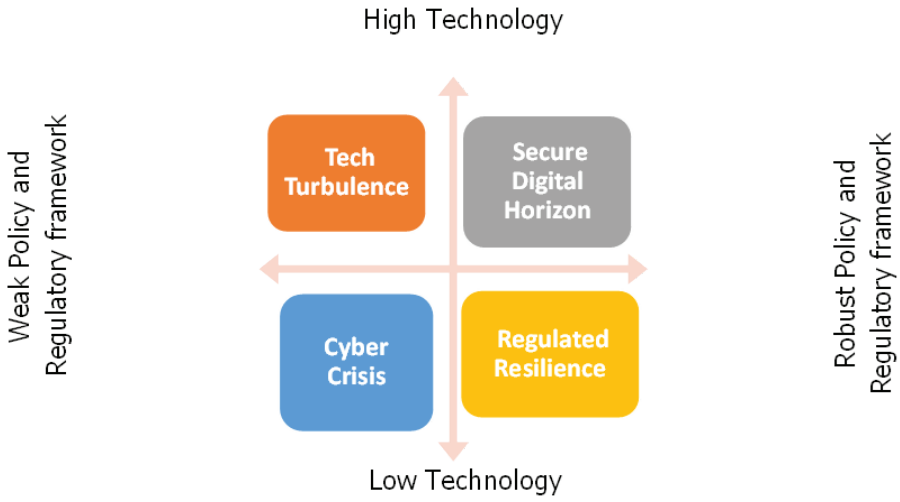
Dynamic nature of technology, integration of security technologies, machine learning and process automation act as relay factors in influencing cyber security. These factors play a critical supportive role in the future of cyber security. Dynamic nature of technology is the strongest relay factor because it has the highest influence and dependency compared to the other relay factors. From the analysis of this study, cloud computing is the most important result factor because it has the highest independence compared to other factors. These other resulting factors are Data encryptions, cyber warfare, and electronic commerce. Autonomous factors from the study findings were internet of things, artificial intelligence and user behavior change. These factors do not have much influence on cyber security.

6.4 Cyber Security Future Scenarios

Scenarios aim to help us prepare for different futures. They help in identifying a probable future., that is plausible and can be believed in. they give emphasis on how our actions today shape the future. this means that we have control of the outcomes that will occur in the future (Bradfield et al. 2005; Schwartz 2012). The scenarios prompt the actions to be taken to shape the future in a way we want it to look like. This as illustrated in the figure below.

Possible Scenarios

Figure 5.3: Future scenario



Secure Digital Horizon

This illustrates the current cyber security situation. Kenya has made great technological progress and established a strong cybersecurity regulatory framework. Businesses are thriving due to confidence in online trade, the business

environment is attracting foreign investors and therefore boosting the economic performance. As a result of these advancements, the nation is now recognized as one of Africa's top tech hubs as envisaged in Vision 2030, guaranteeing the safety of digital infrastructure, safeguarding personal data and promoting a robust digital economy. In this scenario, internet infrastructure is highly developed, with widespread 5G connectivity, advanced fiber-optic networks, and smart city technologies, artificial intelligence and machine learning are extensively used for threat detection and response, enhancing the ability to predict and mitigate cyber-attacks.

In this scenario, blockchain is employed for secure transactions, ensuring data integrity and transparency in various sectors, including finance, healthcare, and supply chain management. With the proliferation of IoT devices, robust security protocols are in place to prevent unauthorized access and ensure the privacy of data transmitted through these devices. There is also a dedicated national agency oversees the implementation of cybersecurity policies, coordinates response efforts, and conducts regular audits of critical infrastructure. This scenario also depicts collaborations between the government and private sector stakeholders to share threat intelligence, conduct joint training exercises, and develop best practices for cybersecurity. There is also collaboration between different countries to ensure that the cyber space is secure.

This scenario depicts a situation where there is smooth flow of online activities due to unavailability of cyber threats. It is a scenario where most of the government and private sector services are conducted online seamlessly without fear of any interruption or cases of data breaches all financial institutions have fully embraced mobile banking, and digital payments, Kenya's financial sector thrives, attracting global investors and fostering economic growth. In this scenario the country has established a safe and thriving digital environment due to its dedication to utilizing cutting-edge technology and putting in place a robust regulatory framework. The country continues to be a resilient and inventive country, setting an example for other nations in the region, by consistently adjusting to new threats and promoting a culture of cybersecurity awareness.

Regulated Resilience

In this scenario, the country has a robust cybersecurity legal and regulatory framework, but the overall level of technology adoption and infrastructure remains low. Despite these technological limitations, the country strives to ensure the security of its digital environment through effective regulation and strategic initiatives. In this scenario, the internet infrastructure is functional but limited, with low broadband coverage and reliance on 3G/4G networks. There is a significant urban-rural divide in access to digital services. Adoption of advanced technologies such as AI, blockchain, and IoT is slow the total adoption being below 50 percent.

Technological adoption in the country is at 38 percent. Also, many processes remain manual or semi-automated, and digital literacy among the population is

relatively low. Strong cyber security laws covering data protection, privacy, digital identity, and cybercrime, have been enacted providing a solid legal foundation for cybersecurity. There are also government collaborations with the private sector, NGOs, and international partners to bridge technological gaps by sharing knowledge and resources. There are few e-government services that concentrate on basic services. Strict laws guarantee the security of these services, despite their limitations.

This scenario shows a country with strong legal and regulatory framework that plays a key role in maintaining cybersecurity despite the low level of technology adoption. Through effective regulation, public-private partnerships, capacity building, and international cooperation, the country strives to secure its digital environment. While technological limitations pose challenges, the country's commitment to cybersecurity and proactive measures ensure resilience against cyber threats, fostering a safe digital ecosystem for the citizens and businesses.

Cyber Crisis

Under this scenario, internet infrastructure is underdeveloped, with limited broadband coverage and reliance on outdated 3G/4G networks. The digital divide between urban and rural areas is pronounced. Adoption of the 4IR technologies like AI, blockchain, and IoT is 3D, ecommerce, e-mobility is minimal. This scenario is also characterized by few initiatives to train cybersecurity professionals or educate the public on cybersecurity best practices, inadequate legal and regulatory framework, with outdated laws governing data protection, privacy, digital identity, and cybercrime.

There is also limited interactions and collaboration between the government and private sector are limited and inadequate resulting to fragmented and uncoordinated cybersecurity. This makes the financial sector struggles with frequent cyber-attacks because of lack of secure digital banking infrastructure and weak regulatory oversight. Cyber fraud and data breaches are common. E-government services are low due to high cyber-attacks rates which makes the public low trust in digital platforms. The business environment is unfavorable to investors affecting the economic performance of the country. The countries' low technology adoption combined with a poor regulatory framework creates a challenging cybersecurity landscape. This combination leaves the country vulnerable to cyber threats, undermining economic growth, public trust, and national security.

Tech Turbulence

This scenario presents a country with extensive high-speed internet coverage, including widespread 5G networks and advanced fiber-optic connectivity. Smart city technologies are prevalent in urban areas. The country has fully embraced 4IR technologies like AI, machine learning, blockchain, IoT, and cloud computing across various sectors, driving innovation and efficiency. There is also a robust

digital economy, which has a thriving fintech sector, e-commerce, digital health services, and e-mobility.

However, there are inadequate cyber laws to govern data protection, privacy, digital identity, and cybercrime. This scenario, banking sector, despite leveraging advanced technologies, are frequent targets of cyber-attacks due to inadequate regulatory oversight and enforcement. This leads to financial losses, fraud, and low consumer trust. E-government services are prone to cyber threats, resulting in data breaches, service disruptions, and loss of public trust in them. Online business is curtailed by fear of cyber-attacks due to lack of regulation.

7. Conclusion and Policy Recommendations

7.1 Conclusion

In the wake of the Fourth Industrial Revolution, cybersecurity in Kenya stands at a critical path where technological advancements and the legal and regulatory framework emerge as the most significant influencers. This paper has explored how the integration of cutting-edge technologies, such as artificial intelligence, the Internet of Things, blockchain, and advanced digital connectivity, brings both opportunities and formidable challenges to the nation's cybersecurity landscape.

The rapid adoption of 4IR technologies has revolutionized various sectors in Kenya, from finance to education and public services. These advancements have driven economic growth, improved efficiency, and increased access to services. However, they have also expanded the attack surface for cyber threats, making cybersecurity a great concern. The increase in interconnected devices and systems introduces new vulnerabilities that can be exploited by cybercriminals, demanding robust cybersecurity measures to safeguard the nation's digital platforms.

A robust legal and regulatory framework is essential to mitigate the risks associated with these technological advancements. The current state of cybersecurity laws in Kenya reveals gaps and inadequacies that leave the country vulnerable to cyber-attacks. Comprehensive and up-to-date legislation, effective enforcement mechanisms, and coordinated efforts across sectors are imperative to enhance national cyber resilience. The establishment of a dedicated national cybersecurity agency, regular updates to cybersecurity laws, and fostering public-private partnerships are critical steps toward building a secure digital environment.

The interplay between technological advancement and regulatory frameworks is crucial. Advanced technologies require equally advanced regulatory measures to manage risks effectively. A strong legal framework can foster innovation by providing clear guidelines and assurances to businesses and individuals. This symbiotic relationship is fundamental to achieving a secure and prosperous digital future for Kenya.

7.2 Policy Recommendations

For the country to be able to be at the secure digital horizon scenario in the next 10 years, the following recommendations can be considered by the stakeholders.

(i) Ensure regular update and review of cybersecurity laws and policies to adapt to the evolving threat landscape and technological changes, and that these laws align with global best practices and standards in addressing emerging threats. The reviews can be done annually.

(ii) Incorporation of cyber security training in early learning curriculum through institute of curriculum development that equips the future generation so that as they adopt the new technology one can also be able to be aware about their security.

(iii) There is need for open collaborative, coordinated and integrated regimes at the operational, technical and policy levels. This will fight against cybercrime, in cyber security, management of scarce resources and in the delivery of all the other programs and projects.

(iv) Resource mobilization towards cyber security to enable employ cyber security experts and required infrastructure to detect and prevent cyber-attacks.

(v) Identify critical infrastructure sectors such as finance, healthcare, and energy, and develop targeted cybersecurity measures to protect them.

(vi) Increase investment in expanding and upgrading internet infrastructure, focusing on reducing the urban-rural digital divide. This includes improving broadband access and transitioning from outdated 3G/4G networks to more reliable connections.

(vii) Develop and promote cybersecurity training programs for government officials, law enforcement, and the judiciary to ensure they understand the complexities of cyber threats and can effectively enforce laws.

References

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2).

Alipour, M., Hafezi, R., Amer, M., and Akhavan, A. N. (2017). A new hybrid fuzzy cognitive map-based scenario planning approach for Iran's oil production pathways in the post–sanction period. Energy, 135, 851-864.

Ansari, M. F., Dash, B., Sharma, P., and Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering.

Chitechi, K. V., Omieno, K. K., and Mbugua, S. (2021). Cyber-Security Vulnerability Assessment Model for County Governments in Kenya. International Journal of Science and Research (IJSR), 10(7), 792-797.

Chizanga, M. K., Agola, J., and Rodrigues, A. (2022). Factors affecting cyber security awareness in combating cybercrime in Kenyan public universities. International Research Journal of Innovations in Engineering and Technology, 6(1)

Cinini, S. F., Ehiane, S. O., Osaye, F. J., and Irewunmi, B. A. (2023). The Trends of Cybersecurity and Its Emerging Challenges in Africa. In Cybercrime and Challenges in South Africa (pp. 75-106). Singapore: Springer Nature Singapore.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., and Atlanta, G. A. (2008). Cybersecurity in africa: An assessment. Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.

Cooper, R. B. and Zmud, R. W., 1990. Information Technology Implementation Research: A Technological Diffusion Approach. Management Science, 36(2), pp. 123-139.

D'Adamo, I., González-Sánchez, R., Medina-Salgado, M. S., and Settembre-Blundo, D. (2021). E-commerce calls for cyber-security and sustainability: How European citizens look for a trusted online environment. Sustainability, 13(12), 6752.

Fielder, J. D. (2021). Cyber security in Kenya: Balancing economic security and internet freedom. In Routledge Companion to Global Cyber-Security Strategy (pp. 543-552). Routledge

Ghasemian, S., Faridzad, A., Abbaszadeh, P., Taklif, A., Ghasemi, A., and Hafezi, R. (2020). An overview of global energy scenarios by 2040: identifying the driving forces using cross-impact analysis method. International Journal of Environmental Science and Technology, 1-24

Ghelani, D. (2022). Cyber security, cyber threats, implications and future

perspectives: A Review. Authorea Preprints

Gordon, A. (2010). A DEFT approach to trend-based foresight. Foresight, 13-19.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., and Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business and Economics, 3(5), 97.

International Telecommunication Union. (n.d.). Cybersecurity. Retrieved June 7, 2024, fromhttps://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx

Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993

Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.

Jhanjhi, N. Z., Humayun, M., and Almuayqil, S. N. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. Computer Systems Science and Engineering, 37(3).

Kaibiru, R. M., Karume, S. M., Kibas, F., and Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. Journal of Information Security, 14(2), 136-151.

Kang, J., and Westskytte, S. (2018). Diffusion of Cybersecurity Technology-Next Generation, Powered by Artificial Intelligence.

Kenya National Bureau of Statistics. (2024). Economic survey 2024. Kenya National Bureau of Statistics.

Li, Y., and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., and Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology, 13, 927398.

Mugarura, N., and Ssali, E. (2021). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. Journal of Money Laundering Control, 24(1), 10-28.

Muhati, E. (2018). Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises (Thesis). Strathmore University. Retrieved from http://suplus.strathmore.edu/handle/11071/6013

Mwangi, T., Asava, T., and Akerele, I. (2022). Cybersecurity Threats in Africa. In The Palgrave Handbook of Sustainable Peace and Security in Africa (pp. 159-180). Cham: Springer International Publishing.

Ngare, B. M. (2018). FACTORS CONTRIBUTING TO CYBER SECURITY FRAMEWORK IN KENYA: A case STUDY OF KENYAN TELECOMMUNICATIONS COMPANIES. GSJ, 6(3), 156

Parn, E. A., and Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. Engineering, Construction and Architectural Management, 26(2), 245-266.

Pillkahn, U. (2008). Using trends and scenarios as tools for strategy development: shaping the future of your enterprise. John Wiley and Sons.

Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., and Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of manufacturing systems, 58, 176-192.

Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: A Case Study of Kenya (Doctoral dissertation, university of Nairobi).

Samoei, P. C., and Gatobu, P. (2024). CYBERSECURITY AND PERFORMANCE OF INTERNET BANKING SERVICES IN COMMERCIAL BANKS IN NAIROBI CITY COUNTY, KENYA. International Journal of Social Sciences Management and Entrepreneurship (IJSSME), 8(1).

Sarker, I. H., Furhad, M. H., and Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series, 33, 2020-01.

Taddeo, M., McCutcheon, T., and Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557-560.

Taddeo, M., McCutcheon, T., and Floridi, L. (2021). Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword. Ethics, Governance, and Policies in Artificial Intelligence, 289-297.

Yaacoub, J. P. A., Noura, H. N., Salman, O., and Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 1-44.

Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., and Ayassrah, A. Y. B. A. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. Heliyon, 10(1).

ISBN 978 9914 738 65 0

Kenya Institute for Public Policy Research and Analysis
Bishops Garden Towers, Bishops Road
PO Box 56445, Nairobi, Kenya
tel: +254 20 2719933/4, 2714714/5, 2721654, 2721110
fax: +254 20 2719951
email: admin@kippra.or.ke
website: http://www.kippra.org