Challenges of Cybersecurity Resilience in Uganda: A Case of Uganda Police Force

Barisigara Paul Wyclef

2023/HD03/28036U

2300728036

A Research Report Submitted to the Directorate of Research and Graduate Training

in Partial Fulfillment of the Requirements for the Award of a Master of

Arts Degree in Defense and Security Studies of

Makerere University

June, 2025

DECLARATION

I, **Barisigara Paul Wyclef**, Reg. No. **2023/HD03/28036U,** declare that this research report titled: "**Challenges of Cybersecurity Resilience in Uganda: A Case of Uganda Police Force**", has not been presented for any degree award in any other university.

Signature..... Date..28 JULY 2023.....

Barisigara Paul Wyclef

2023/HD03/28036U

APPROVAL

This is to certify that this research titled: **"Challenges of Cybersecurity Resilience in Uganda: A Case of Uganda Police Force"**, has been developed under my guidance.

Signature..... Date.....23/7/25.....

Dr. Solomon Winyi

(Supervisor)

Dedication

I dedicate this research report to my wife, Agaba Aisa, for her continued support, encouragement to work hard, my son Baris Aiden and friends for the advice, guidance and physical support rendered to me during the time of my research work.

Acknowledgements

I would like to thank the Ministry of Defence and Veteran Affairs for sponsoring me to undertake this postgraduate degree of Masters of Arts in Defence and Security Studies (MDSS) of Makerere University, Kampala.

Table of Contents

List of Abbreviations

AFRIPOL	The African Union Mechanism for Police Cooperation
AI	Artificial Intelligence
AU	African Union
CCPA	California Consumer Privacy Act
CERTs	Computer Emergency Response Teams
CERTs	Computer Emergency Response Teams
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CPSs	Cyber–Physical Systems
DDoS	Distributed Denial of Service
DFIR	Forensic Incident Response
EAPCCO	East African Crude Oil Pipeline
GDPR	General Data Protection Regulation
GoU	Government of Uganda
HR	Human Resource
HRM	Human Resource Management
IEC	International Electrotechnical Commission

IoT	Internet of Things
ISMS	Security Management Systems
ISO/IEC	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
ML	Machine Learning
NIST	National Institute of Standards and Technology
NITA-U	National Information Technology Authority, Uganda
RE	Resilience Engineering
U. S	United State
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UPF	Ugandan Police Force
WB	World Bank

Abstract

The study examines the ongoing difficulties that compromise cybersecurity resilience in the Uganda Police Force (UPF), emphasising the relationship between technological infrastructure development and human resource competencies. Routine Activity Theory posits that a crime transpires when motivated criminals, suitable targets, and the absence of capable guardians converge. The study rigorously analysed the impact of systemic vulnerabilities on the Uganda Police Force's capacity to protect its digital ecosystem as a custodian. The core issue lies in the disparity between swift technological adoption and insufficient institutional readiness, which renders essential security infrastructure vulnerable to cyber threats that the UPF is presently ill-prepared to address thoroughly. A qualitative desk review approach was employed to synthesise data from diverse secondary sources, including peer-reviewed journals, government papers, policy documents, and news items. Research indicates that although the technical infrastructure in the UPF, including digital databases, communication systems, and surveillance technologies, has enhanced operating efficiency, it is still inconsistent, fragmented, and inadequately guarded, frequently lacking integrated cybersecurity measures. Simultaneously, despite initiatives to create cybercrime units and provide fundamental training, the UPF still faces a deficiency of specialised staff, restricted advanced skills, and a lack of organised professional growth avenues in cybersecurity. The deficiency of human resources significantly undermines the organization's capacity to identify, react to, and recuperate from cyber threats in real time. The study indicates that although the UPF has aligned certain practices with international cybersecurity standards however Uganda has not ratified to the most vital conventions of cyber security. These concerns cumulatively undermine the resilience and Uganda's conformity to international norms in the areas of cyber security. The main recommendations are increased funding to procure latest technology to combat the increasing cyber crimes and Uganda to ratify to the most important conventions to get international collaborations and trainings.

Key words; Challenges, Cybersecurity, Resilience and Uganda Police Force.

CHAPTER ONE

INTRODUCTION

1.0. Introduction.

Uganda, like many nations undergoing digital transformation, is increasingly grappling with serious cybersecurity challenges. Among the most pressing are a surge in phishing scams, many of which are now powered by artificial intelligence. These attacks have become more sophisticated and personalized, often targeting individuals and institutions by mimicking trusted communications to extract sensitive data. The consequences of such cyber threats are severe ranging from financial losses and operational disruption to reputational damage and erosion of public trust. As a vital institution responsible for national security and public order, the Uganda Police Force (UPF) finds itself at the frontline of both responding to and being targeted by such cyber incidents. However, its preparedness and resilience in the face of these evolving threats remain uncertain and underexplored.

To explore these issues in the Ugandan context, this study adopts a qualitative desk review methodology, drawing data from existing scholarly literature, policy documents, government reports, media articles, and institutional records. This approach allows for a comprehensive synthesis of current knowledge on the UPF's cybersecurity posture, infrastructural capabilities, and institutional strategies in relation to global norms. This introductory chapter sets the stage for the study by presenting the background, problem statement, purpose of the study, research questions, scope, and significance.

1.1 Background

In today's connected and digital world, cybersecurity is a problem for everyone, but it's especially important for countries like Uganda that are quickly catching up with technology. It is more important than ever to keep our data safe, whether it is personal or not, and to keep the digital infrastructure safe as we use digital technologies more and more for everyday tasks. Because of this, cybersecurity is now a big part of modern data governance. To keep digital assets safe and lower risks to the infrastructure, it needs a lot of different methods. Digital technology is becoming more and more important for communication, governance, business, and

national security (Anderson & Thompson, 2015; Taylor & Wilson, 2020). But as we use more and more digital technology, we also become more vulnerable to cyber threats like ransomware, data breaches, phishing attempts, and systemic digital espionage.

By 2025, the International Telecommunication Union (ITU, 2022) predicts that worldwide cybercrime losses will reach USD 10.5 trillion per year, underscoring the need for countries to not only prevent cyberattacks but also develop the capacity to withstand, respond to, and recover from them—a concept known as cybersecurity resilience (Chen & Wang, 2018). According to Hunton (2011), cybercrime is commonly defined as a global phenomenon that includes illegal activity as well as other undesirable behaviours that make use of networked technology. Cybercrime is defined as the utilisation of networked computers or Internet technologies to perpetrate or facilitate criminal activities (Gilmour, 2014). According to the European Commission (2013), "cybercrime typically denotes a wide array of criminal activities in which computers and information systems serve either as the principal instrument or as the main target." Traditional crimes like fraud, forgery, and identity theft are included in cybercrime, as are content-related crimes like online child pornography distribution and inciting racial hatred, as well as offences unique to computers and information systems like malware, denial of service attacks, and information system attacks (Gilmour, 2014).

Cybersecurity is the term for the steps that need to be taken to protect network and information systems, their users, and other people who are affected by cyber threats. Many countries are now spending a lot of money on it (European Parliament and Council, 2019). This definition makes it clear that cybersecurity is a very broad field that includes protecting people and society as well as technology and data. It stresses how important it is to have strong defences against a wide range of cyberthreats that can affect many areas of life, from personal privacy to national security.

To deal with cybersecurity problems, we need more than just the right technology; we also need a full legal framework that can adapt to the changing threat landscape. It is widely agreed that law is very important for cybersecurity. Bozgeyik (2023) talks about how important it is for people, businesses, and governments to have legal protections against different types of

cyberthreats. These threats include cybercrimes, privacy violations, intellectual property theft, and problems with international relations. Joshi (2024) also talks about how important it is for cybersecurity laws and rules to change to keep up with new threats. He stresses the importance of global cooperation and ongoing legislative evolution to keep up with how quickly technology is changing. Solove and Hartzog (2022) say that data security law should take a more holistic approach, stressing the need to focus on the whole data processing system and make sure that everyone in the ecosystem is responsible. They want the law to focus on preventing and reducing data security problems instead of reacting to them.

Many countries and regional groups have changed or made new cybersecurity laws in response to rising cyberthreats. These rules set the standards for cybersecurity that businesses must follow to protect their data and systems. The General Data Protection Regulation (GDPR) (European Parliament and Council, 2016) says that personal data must be protected by appropriate technical and organisational security measures. These rules set a basic level of protection for information assets and require penalties for not following them. They also encourage strict cybersecurity procedures. They define and make illegal cyber crimes like hacking, accessing computers without permission, and cyber fraud. This makes cybercriminals less likely to commit these crimes and gives the police a legal basis to arrest them. Some countries have taken the initiative to pass and update laws to deal with cybersecurity threats, while others have fallen behind. Uganda is one of the latter types; its cybersecurity laws haven't kept up with the growth of its digital economy, even though it is slowly building one.

The Computer Misuse Act, which was passed in 2011, is part of Uganda's current cybersecurity framework. This law is meant to stop people from getting into computers and computer systems without permission, even if they use harmful software. It makes things like hacking, intercepting data, and misusing computer systems illegal. This encourages people to use computers responsibly and protects them from cybercrimes. With this law, Uganda wants to make the internet a safe place for people and businesses to do business. the Because of this, the country's cyber defence needs to be strengthened by changing the rules and taking a comprehensive, law-based approach. The Data Protection and Privacy Act of 2019 is another important law that stresses the need to protect personal data and privacy rights. This law sets out the rules for how

personal data can be processed. It says that data controllers and processors must take the necessary steps to keep the data safe. The Act also gives people rights over their personal information, which is a key part of the country's cybersecurity plan. Lastly, the Electronic Transactions Act is just as important because it makes electronic transactions legal and makes it easier for people to buy and sell things online in Uganda. This law, which went into effect in 2011, protects the integrity and security of electronic communications, which builds trust in digital transactions. It talks about things like electronic signatures and whether electronic evidence can be used in court, which are important for running cyber operations smoothly. So, Uganda needs to change its rules and take a more comprehensive, law-based approach to strengthening the country's cyber defence.

But the rules above need to be changed a lot to keep up with how complicated and advanced modern cybercrimes and cybersecurity are. For example, when the Computer Misuse Act was passed, the crimes it dealt with were common. Since then, new cybercrimes have appeared, and some are still changing. Some parts of the Act could be changed to cover new types of cybercrime, but it's not clear if the Act is flexible and adaptable enough to deal with new threats like revenge porn, disinformation, deepfakes, and ransomware (Nwafor et al., 2021; Ajayi, 2023). It is very important in criminal law to know exactly what crimes are. If you change the definitions that are already in use, it might make things less clear and make it harder for justice to be served. The punishments in the Cybercrimes Act aren't strong enough to stop these crimes from happening either. A lot of its fines are much lower than the damage that cybercrime can do to people and information systems (Sibe, 2024).

The laws are insufficient because cybercrime has increased in Uganda as a result of the country's rapidly expanding digital landscape. Uganda's internet and bandwidth usage has significantly increased. From 91.4 million gigabytes in 2022 to 138.5 million gigabytes in 2023, there has been a 51% increase in internet traffic. This indicates that Ugandans have incorporated the internet into their everyday routines. Sixty-four percent of people use the Internet as of December 31, 2023. There are currently 27 million Internet subscribers and 34.3 million mobile phone users. Currently, there are 26 million active mobile money accounts out of 37.3 million total. This demonstrates the potential utility of digital payments. A staggering Shs 54.5 trillion

has been transferred via mobile money. This volume of transactions is significantly more than what has been conducted by traditional banking for more than a century. To set the scene, mobile money was first introduced in 2009[1].

Resilience has become a popular idea over the years and is used in many fields, even though there isn't a single definition of it (Rogers, 2020; Smith, 2023; Araujo et al., 2024). This is because laws can't stop cybercrime. In the field of cybersecurity, it is widely accepted that a comprehensive approach to security includes an organization's ability to proactively prepare for, detect, respond to, mitigate, and recover from a cyber incident in order to minimise the impact on its systems and services (Cisco, nd; IBM, nd). It has a lot of different ways to keep things running smoothly when there are cyberthreats. These strategies include more than just protection and defence; they also include being ready, being flexible, and recovering (AL-Hawamleh, 2024). The most important cybersecurity groups say that cyber resilience is the ability to predict, survive, bounce back from, and change in response to cyber incidents. Ross et al. (2021, p. 1) say that it is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Being able to predict, stop, find, respond to, and recover from cyber incidents are all important parts of cyber resilience.

In Uganda, digitisation is very important in the fight against cybercrime, especially in the Kampala metropolitan area and other cities across the country. The Ugandan government has made a number of improvements to security using technology, as well as e-governance platforms and digital banking systems (Mugisha & Namanya, 2020). To make policing more effective and

1 JJingo Ernst, 2024. Govt has developed capacity to tackle all cyber security issues – PS Zawedde. The Observer newspaper. https://observer.ug/news/govt-has-developed-capacity-to-tackle-all-cyber-security-issues-ps-zawedde/

keep the country safe, the Uganda Police Force (UPF) has started using digital surveillance systems, online crime reporting platforms, and biometric data systems (Harris & Lee, 2017). Some of the new technologies are: CCTV cameras set up in major cities to stop crime and respond to it; digital number plates that make it easier to track and hold people accountable for their actions; national biometric systems that help identify citizens and law enforcement; and the integration of police databases with INTERPOL systems for cross-border crime intelligence (Parker & Quinn, 2018).

These digital tools are a big step forward, but they also add new layers of cybersecurity risk. Some evidence has shown that these infrastructures have problems with unauthorised access, data breaches, system downtimes, and not properly integrating cybersecurity protocols. For example, Uganda's CCTV camera system, which is very big, has been criticised for having weak cybersecurity measures that could make the network vulnerable to cybercriminals or hostile actors (Katureebe, 2022). The use of digital number plates to stop crime also raises concerns about data privacy, encryption standards, and the integrity of the central system if they are not properly protected.

Even though the tools are very advanced, Uganda still has a lot of problems with cybersecurity resilience, especially in public security organisations like the UPF. Infrastructural problems and a lack of skilled workers are often to blame for these problems (Mbabazi, 2023). The Uganda Police Force has done a great job of using technology, but three big problems make its cybersecurity less strong: Many of the digital tools that have been adopted, like surveillance systems, databases, and communication tools, work in silos and don't have centralised coordination or standardised cybersecurity controls. The system is vulnerable to internal weaknesses, unauthorised access, and poor threat detection because there is no strong and unified IT governance framework (Moyo & Ndlovu, 2008). Cybersecurity in law enforcement needs more than just IT experts; it also needs people who are trained in digital forensics, threat intelligence, and incident response. But the UPF doesn't have enough specialised cybersecurity staff and only a few programs that offer ongoing training. A lot of the time, current employees don't know about the latest threats or protocols that are in line with global cybersecurity standards. Uganda has passed cyber laws like the Computer Misuse Act and made national

cybersecurity plans, but they are still not being put into action by institutions. The Uganda Police Force does not have an internal cybersecurity plan that follows international standards like ISO/IEC 27001 or NIST. This means that it is reactive instead of proactive (Mugisha & Namanya, 2020).

The Uganda Police Force is using more and more digital tools to keep the country safe. This makes the gap between how quickly technology is changing and how prepared institutions are for cyberattacks even more dangerous (Osei & Asante, 2020). The UPF is in danger of systemic digital threats because its infrastructure isn't well-coordinated, it doesn't have enough skilled workers, and its cybersecurity systems aren't flexible. There are global and regional plans to make cybersecurity stronger, but Uganda's internal security agencies don't always follow them. This study wanted to look at these basic structural and capacity-based problems and see how they affect the Uganda Police Force's ability to protect itself from cyberattacks.

1.2 Statement of the Problem

Even though Uganda has made significant progress in developing the legal and regulatory environment for digital transformation, developing e-services and improving cyber security, more efforts to improve the digital landscape are still required. Existing laws still exhibit limited scope and coverage, failing to adequately address cybersecurity holistically across all sectors and neglecting the crucial aspect of cyber resilience. The other challenge besides the limited laws, is the resource and skills gaps impede effective development and implementation.

Uganda has not kept up with the pace of the evolving challenges in digital technologies related to governance and law enforcement, regulatory and technical frameworks for cybersecurity (NITA-U, 2021). The government’s digital transformation in the Uganda Police Force (UPF) has been marked by investments in Closed-Circuit Television (CCTV) cameras, smart policing tools, and planned rollouts of digital number plates. These tools are aimed at enhancing surveillance, evidence collection, and crime prevention. However, these advancements have outpaced the growth of Uganda’s cybersecurity capabilities, leaving critical security infrastructure exposed to cyber threats. According to the International Telecommunication Union (ITU, 2022), Uganda

ranks 91st globally in the Global Cybersecurity Index (GCI), a reflection of its limited policy development, institutional capacity, and response mechanisms.

Further compounding the problem, a 2021 Uganda Communications Commission (UCC) report indicated that over 60% of public sector institutions, including law enforcement, lacked updated cybersecurity policies and incident response frameworks. The 2022 National Information Technology Authority Uganda (NITA-U) report revealed systemic weaknesses in Uganda's cyber landscape, including low public awareness, chronic underfunding, lack of skilled personnel, weak encryption protocols, and poor inter-agency coordination (Uganda Police Force, 2019). These challenges have resulted into an increase in cyber intrusions, data breaches, and targeted attacks on security databases. These incidents not only expose sensitive information but also disrupt critical security operations and erode public confidence in digital governance. These have been caused glaring gaps in digital forensics training, data protection, cyber incident handling, and integration with national Computer Emergency Response Teams (CERTs). This research, therefore, seeks to examine the institutional, legal, technical, and operational challenges of cybersecurity resilience within the Uganda Police Force.

1.3 General Objective of the Study

The general objective of this study is to examine the challenges of cybersecurity resilience in the Uganda Police Force.

1.4 Specific Study Objectives

The study was guided by the following study objectives:

i. To examine the effect of technological infrastructural development on cybersecurity resilience in the Ugandan Police Force.
ii. To examine the influence of human resource capabilities on cybersecurity resilience in the Ugandan Police Force.
iii. To examine the conformity of cybersecurity resilience practices to international norms by the Uganda police.

1.5 Research Questions

The study sought answers to the following research questions:

i. What is the effect of technological infrastructural development on cybersecurity resilience in the Ugandan Police Force?
ii. What is the influence of human resource capabilities on cybersecurity resilience in the Ugandan Police Force?
iii. To what extent do cybersecurity resilience practices in the Ugandan Police Force conform to international norms?

1.6 Scope of the Study

1.6.1. Geographical scope

The Kampala Metropolitan Area, which is a key part of the Uganda Police Force, was the main focus of this study. Kampala was chosen because it is Uganda's economic, political, and technological centre, as well as the centre of cybercrime, especially in wealthy neighbourhoods and business districts like Kololo, Nakawa, Bugolobi, and the Central Business Districts. The Daily Monitor (2023) says that Kampala has seen a rise in cyber-enabled crimes like SIM card swapping, bank fraud, online scams, phishing attacks, and hacking of government websites. These crimes have a bigger impact on private companies and public agencies based in the capital. The study focused on four main departments of the Uganda Police Force (UPF) that are directly or indirectly involved in making the country's cybersecurity stronger: Information and Communication Technology (ICT) is in charge of the police's internal digital infrastructure, system security, and keeping up with new technology. Forensic Services Directorate, which looks into cybercrime and digital forensics. The Crime Intelligence, Interpol & International Relations Directorate is in charge of cyber intelligence, coordinating cross-border crime, and working with groups like INTERPOL and AFRIPOL. The Research, Planning and Development & Counter Terrorism Directorate is in charge of making plans, assessing threats, and making operational policies about terrorism, including cyber-terrorism threats.

1.6.2. Content Scope

The study's main focus is on the problems that make it hard for UPF to be resilient against cyberattacks. To find out how well UPF can prepare for, withstand, and recover from cyberattacks, we look at resilience from a number of angles: technical, institutional, legal, and

strategic. The study uses important ideas from Resilience Engineering Theory, which focusses on making systems strong, flexible, and able to learn from mistakes (Hollnagel et al., 2006). Reports like NITA-U (2022) provided empirical data that showed problems with encryption, risk management, and cyber-awareness. UCC (2021) found that more than 60% of security agencies did not have formal cyber response plans, and the ITU Global Cybersecurity Index (2022) ranked Uganda 91st in the world. These two reports show that even though technology is being used, resilience is still low. Turyakira and Nambatya (2022) is another academic study that looked into digital security in public institutions. They found that cyber readiness is greatly hurt by a lack of ongoing training, broken reporting systems, and old digital infrastructure.

1.6.3. Time scope

The study looked at the time from 2011 to 2025, and this looked at key laws passed, from the Computer Misuse Act of 2011, the Data Protection and Privacy Act of 2019, and the Electronic Transactions Act of 2011, and the adoption of digital surveillance tools, such as the introduction of CCTV systems and the government's plans to implement digital number plates and vehicle tracking systems (New Vision, 2022). During this period, notable incidents have underscored the UPF's vulnerability, such as the 2021 hacking of the Uganda Police recruitment portal, which led to data breaches (Observer, 2021), and the leakage of classified intelligence reports in 2022, allegedly due to poor digital safeguards (Chigudu, 2022).

1.7 Justification of the study

The study will provide data-driven insights to guide the UPF, Ministry of Internal Affairs, NITA-U, and policymakers in designing context-specific cyber resilience policies and training frameworks. It will contribute to academic literature by focusing specifically on the institutional, operational, and technical challenges facing the Uganda Police Force in maintaining cybersecurity resilience. Strengthening the cyber resilience of UPF has direct implications for counterterrorism, organized crime prevention, and the protection of national digital infrastructure. The study aligns with national aspirations to modernize public service delivery and promote a secure digital ecosystem. Understanding these challenges will also inform Uganda's engagement with regional cybersecurity initiatives under the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) and with

global agencies like INTERPOL and AFRIPOL. This study is both timely and necessary, offering practical recommendations for building a resilient, responsive, and secure law enforcement digital ecosystem in Uganda.

1.8 Significance of the study.

The study gives real-world proof that the UPF and other security agencies need to make their cybersecurity policies and institutional frameworks better. It points out specific problems with infrastructure, policy, training, and coordination between agencies, and it gives concrete suggestions for how to fix these problems and build up the country's and region's cybersecurity capacity. This study also helps the national cybersecurity agenda by finding the technical and operational weaknesses in the Uganda Police Force. This will help Uganda become better at stopping, finding, and responding to cyber incidents. This is very important for keeping the country stable, stopping crime, fighting terrorism, and keeping digital public services safe

The study helps create targeted training programs for police officers in digital forensics, safe data handling, threat intelligence, and coordinating responses. The Uganda Police Training School, NITA-U, and Uganda Communications Commission (UCC) will use information about current skill and knowledge gaps to create relevant curricula and certification programs. The study will also add to the small amount of academic writing that exists on cybersecurity resilience in policing in sub-Saharan Africa, especially in Uganda. It also connects cybersecurity theory, resilience engineering, and law enforcement practice by providing a model that can be used in future research in criminology, ICT policy, and public administration.

1.9 Theoretical Framework

Cohen and Felson came up with the Routine Activity Theory in 1979. It says that crime happens when three things come together: a criminal who is motivated, a target that is right, and a guardian who is not capable of stopping the crime. This study uses Routine Activity Theory to look at cybercrimes that make it easier for other crimes to happen. This study looks at the problems with human resources and the problems with laws that make it harder for cyber security to be strong. According to theory, crime is likely to happen when a motivated criminal, a

suitable target, and a lack of a capable guardian come together (Cohen and Felson, 1979). In this situation, the problems with cybercrime resilience let determined criminals take advantage of the situation because there is no skilled guardian, such as the Ugandan police, who are limited by a lack of regulatory enforcement and the necessary skills.

There are probably a number of reasons why RAT was chosen as a "test case" for how criminological theory can be used to cybercrime. This is a well-known and widely used theory for looking at different types of crime, such as burglary (Cohen and Felson, 1979), murder (Messner and Tardiff, 1985), car theft (Rice and Smith, 2002), and domestic violence (Mannon, 1997). Second, its own analytical framework makes it easy to use in a lot of different situations. Third, it gives clear advice on crime prevention and policy, as shown by "situational crime prevention" programs that use Routine Activity Theory (RAT). At first, people talked about how well RAT worked for cybercrimes by looking at how virtual and physical environments are similar and different, as well as how online and offline behaviours are similar and different. But you can't be sure how well a theory explains things until you put it into practice.

As a result, studies of cybercrime that try to use Routine Activity Theory to different types of online crime have recently added to theoretical discussions. Cohen and Felson (1979) said that people are more likely to be victims when they are in high-risk situations, are appealing targets, don't have a good guardian, and are close to a motivated criminal. RAT focusses on the crime itself instead of the person who did it. This is especially important when looking at cybercrime because it's hard to get to know cybercriminals to study their motivations because they don't get caught very often. On the other hand, cybercrime incidents happen all the time and leave digital signatures that can be used for research. Newman and Clarke (2003) were pioneers in applying Routine Activity Theory (RAT) to cybercrime, positing that the accessibility of Internet targets (augmented by the lack of capable guardianship) and visibility (enhanced by the diversity and frequency of online activities, such as shopping and banking) are distinguishing traits between victims and non-victims of cybercrime.

According to Yar (2005), the basic ideas of Routine Activity Theory show that "motivated offenders" and "competent guardianship" are similar in both cyber and real life. However, putting "appropriate targets" into practice was difficult because the theory says that "the

organisation of time and space is important to criminological explanation" (Felson 1998: 148). This is because cyberspace is characterised by spatio-temporal disorganisation (i.e., the victim and criminal are rarely in the same place at the same time). Eck and Clarke (2003) say that Routine Activity Theory (RAT) can be expanded to explain crimes that happen when the victim and the criminal are not in the same place. It follows that the perpetrator can reach a target through this network if the theory's requirement of a shared physical location is changed to include a "shared network," like the Internet.

RAT has been used in a lot of cybercrimes, but the results have not always been the same. Cyber-harassment was linked to being close to motivated offenders and having a more varied and intense online routine. However, physical security measures like installing anti-virus software were not (Holt and Bossler 2008; van Wilsem 2011; Bossler et al. 2012; van Wilsem 2013a). Using RAT to fix computer virus infections didn't always work. Choi (2008) found a link between online lifestyles and physical guardianship and victimisation. However, Bossler and Holt (2009) found that personal measures, like changing passwords often, were not linked to physical guardianship.

1.10 Research Methodology

The study utilized a descriptive research design to collect qualitative data aimed at exploring the challenges of cybersecurity resilience within the Uganda Police Force. To ensure the relevance and depth of the information, the researcher conducted an extensive desk review of existing literature and documentation. Data was gathered from secondary sources such as government publications, policy documents, journal articles, cybersecurity reports, and academic studies. These sources were systematically examined to identify key patterns, emerging themes, and gaps in the current understanding of cybersecurity resilience in law enforcement. The content analysis method was employed to interpret the data, focusing on trends, thematic insights, and contextual meanings drawn from the texts. This approach allowed the researcher to critically assess the current state of cybersecurity resilience in the Uganda Police Force without the need for primary fieldwork, while drawing conclusions grounded in established knowledge and documented evidence.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter presents a critical review of both theoretical and empirical literature relevant to the study, focusing on the relationship between the key study variables. The review is organized thematically in accordance with the specific objectives of the study**,** enabling a structured analysis of existing knowledge and scholarly debates surrounding cybersecurity resilience, particularly within law enforcement contexts. The chapter not only synthesizes current literature but also identifies gaps, inconsistencies, and limitations in previous research, thereby highlighting areas where further investigation is needed. In doing so, the review provides a solid foundation for the present study and justifies its relevance within the broader academic and policy discourse on cybersecurity in Uganda and similar developing contexts.

2.1 Theoretical Debates on Cyber security resilience

Smith and Stamatakis (2020) say that the Routine Activity Theory and Rational Choice Theory have been changed a little bit to fit cyber settings. Still, they are based on traditional criminology, which focusses on crime that happens by chance. These ideas say that a crime happens when motivated criminals, suitable victims, and a lack of skilled guardians come together. They explain the conditions that could lead to cyberattacks, but they don't go into detail about how cyber-physical systems work or the many reasons why attacks on critical infrastructure happen (Fischerkeller et al., 2022; Uribe et al., 2020). The Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM) focus on the psychological and user acceptance aspects of technology and security protocols (Go et al., 2020; Skalkos et al., 2023). These factors are important for understanding how people and organisations act when it comes to cybersecurity, but they don't take into account how cyber-physical systems in critical infrastructure are connected (Khan et al., 2022). The research by Moznik et al. (2023) stresses the need for a comprehensive model that combines cyber and information security to effectively deal with the changing threat environment, which PMT and TAM do not fully cover.

According to routine activity theory developed by Cohen and Felson (1979), motivated offenders and suitable targets will meet more frequently in time and space due to changes in opportunity situations (such as an increase in online users) and a lack of capable guardianship. According to Pratt et al. (2010), "this theory focusses on the behaviours, activities, and situational contexts that put would-be targets at risk for victimisation and assumes a constant supply of motivated offenders." Routine activity theorists claim that when it comes to elucidating patterns or trends in crime, the organisation of social activities varies the most.
Given the frequency of cyberattacks, this theory might be even more pertinent today. Even though more people are using the internet for work, they are not protected by the firewall or security measures of the company. Cybercriminals are believed to be (1) driven by financial gain or criminal activity, (2) seeking opportunities in cyberspace, and (3) targeting poorly secured systems and networks.

According to Cohen and Felson (1979), a motivated offender is a person who possesses criminal tendencies as well as the capacity and desire to commit crimes. Because it assumed that motivated offenders were either common or expected in society, the original framework of routine activities theory failed to define what makes a motivated criminal (Cullen et al., 2018). In their original work, Cohen and Felson identified this flaw and stated that further research was necessary to examine the structural and social factors that can motivate criminal behaviour.
Cohen and Felson's theoretical model is helpful for improving crime prevention strategies as well as for comprehending the reasons behind fraud targeting and victimization[2] . Regarding online fraud, routine activity theory has significant ramifications for crime control tactics. This is due to the fact that potential victims can be educated or informed about how to modify their online conduct in order to prevent becoming victims. Information is a primary target of Internet crime when employing this strategy in cyberspace[3]. Cybercriminals are now targeting databases[4] that contain personal data, such as names, addresses, passwords, and bank account information, because they fit the CRAVED model discussed by Clarke (1999).

[2] Pratt T C, Holtfreter K and Reisig M D 2010 Routine online activity and internet fraud targeting: Extending the generality of routine activity theory Journal of Research in Crime and Delinquency 47 267–96

[3] Newman G R and Clarke R V 2013 Superhighway robbery: Preventing e-commerce crime

[4] Clarke R V. 1995 Situational Crime Prevention Crime and Justice 91–150

End users, technical personnel (such as network administrators), and automated defences like firewalls, virtual private networks, anti-virus and anti-intrusion software, ID authentication, and access management systems are examples of "capable guardians" in RAT (Leukfeldt & Yar, 2016). People who spend a lot of time online, use online banking and shopping more, and engage in activities that put them at risk are more likely to be targeted by criminals (Kigerl, 2012). According to RAT, having capable guardianship is the most important factor in lowering victimisation (Leukfeldt & Yar, 2016). When determining the likelihood of an offence, the presence or absence of guardians at the time and place where acceptable targets and potential offenders meet is crucial.

2.2 Effects of Technological Infrastructural Development on Cybersecurity Resilience

As a technical environment, cyberspace is made up of and depends on digital technology that is always changing because new ideas are widely accepted and spread, changing the way it looks. But focussing only on technology ignores three important parts of cyberspace. At first, like all technology, cyberspace is completely made by people. The way that certain people think and feel has a big impact on how technologies are made and developed. Technologies don't have any inherent meaning, and they don't work alone; they are part of a network of people, ideas, and other things, both physical and non-physical. In addition, economic conditions affect some aspects of technical innovation and the availability of ideas and services that can help reduce certain risks. Second, cyberspace is linked to other systems, like the energy network, and doesn't work on its own. As a result, many important systems depend on each other and need information and communication technology to work. These infrastructures and their interdependencies are very important because they play a key role in society. Third, there are many ways that the basic technology interacts with the people who use it and operate it in cyberspace. Cyberspace is based on how people use technology and how technology connects them. This is especially true for cybersecurity, or the lack of it, which is only important because of how it affects people and their values (Dunn Cavelty, Eriksen, and Scharte, 2023). These three factors make cyberspace a socio-technical system, which is made up of technology, human and social behaviours and interests, and how these parts interact with each other (Sawyer and Jarrahi, 2014).

Peter's (2017) study shows how ready "Africa's top 12 emerging economies" are for cyber resilience and stresses how important it is to be cyber resilient. Many important services, such as emergency services, banking systems, water management systems, electric power grids, and navigation systems for air and sea travel, must now be able to withstand cyberattacks (Dalal et al., 2022; A. Mishra et al., 2022). Cybercrimes and disruptions have proliferated, now impacting critical infrastructure such as energy and telecommunications networks, as well as healthcare facilities (Kovacevic & Nikolic, 2014). Studies show that problems with cyber security resilience are changing as more companies are responsible for keeping up infrastructures, depend on each other, and have a lot of historical context (Cedergren et al., 2018; Niemimaa, 2016).

Recent studies have shown that sustainable smart cities face a lot of complicated problems, such as those related to technology, society, the economy, and the environment. The study gives a thorough look at possible trends and problems that could get in the way of making smart cities(Leroy, Zolotaryova, and Semenov, 2025). The study lists the main problems, such as worries about data privacy, the need for citizen involvement, and the challenges of using renewable energy sources. The authors say that the link between technology and sustainability is very important for city planning. They suggest improving governance systems and making policies that everyone can work on together to make cities more resilient. These results are in line with a lot of discussions about how important it is to combine key infrastructures like energy, transport, and PayTech systems to make smart cities more stable economically and socially (Leroy, Zolotaryova, and Semenov, 2025). PayTech systems set up the financial infrastructure that smart cities need to work. They make it easier to connect to energy, healthcare, and transportation networks, which lets people make safe payments for utilities, transportation, and medical care.

Historically, cybersecurity has placed a strong emphasis on protecting against malicious attacks. Cybersecurity protects organisations' valuable, rare, unique, and non-replaceable (VRIN) data (Lees et al., 2018; Lee, 2021). The idea of cyber resilience has become increasingly important in the last ten years as a key component of managing digital risks. Early cybersecurity guidelines focused on using tools like firewalls to protect a system's internal perimeter. Cyber resilience, on the other hand, focusses on investing in the right technology infrastructure to enable organisations to successfully prepare for, withstand, and recover from inevitable security

breaches (Saeed et al., 2023a). Because information security involves both digital and physical aspects, researchers have worked to improve resilience assessment tools, frameworks, and techniques. Having high-quality technological tools is crucial (Saeed et al., 2023a).

In the rapidly evolving field of information security, the idea of resilience is essential for protecting private information and digital infrastructures (Saeed et al., 2023). Resilience in cybersecurity refers to a system's ability to withstand, adapt to, and recover from unanticipated challenges, such as intrusions, disruptions, and cyberattacks (Gould, 2018). Emerging technologies like cloud computing, blockchain, artificial intelligence, big data and analytics, the Internet of Things, and the industrial Internet of things greatly support technological advancements (Akter et al., 2020; Distor et al., 2023). Because of their many benefits, the technologies used by organisations and other entities are intensifying the push for digital transformation. In order to maintain continuity, entities must safeguard their digital transformation assets from cybersecurity threats.

Advances in technology have prompted a great deal of cybersecurity research to clarify the problem and suggest possible fixes. Three categories of cyber risks make it easier to identify the best course of action and suitable security measures. First, there has been a greater focus on cyberterrorism. It seeks to make the general public fearful and terrified of technology (Weimann, 2014). Extremists who oppose technological advancement use it to cause fear and panic in order to interfere with society's ability to function. Political organisations and the dissemination of private data are the main targets of cyberattacks. In the end, cybercrime targets a variety of systems and is motivated by disruption and financial gain (Ablon, 2018). As technology advances, cyber threats continue to emerge (NIST, 2020). Every technological advancement is accompanied by changes in cyberthreats. Ransomware, malware, and phishing are examples of frequently encountered cyberthreats. These attacks require careful planning because many security measures require physical enclosures to be installed in the devices or structures where data is entered.

According to multiple studies looking into this relationship, police forces' cybersecurity resilience has improved significantly as a result of the development of technological infrastructure. Williams et al. (2016) conducted a study to assess how police departments' ability

to handle cyber threats is impacted by contemporary technology infrastructure and found that those with more sophisticated technological infrastructures—like data centres and real-time monitoring systems—were significantly better at spotting and thwarting cyberthreats. O'Brien and Jenkins (2018) looked at the relationship between police forces' overall resilience and the calibre of cybersecurity infrastructure and findings showed that departments with sophisticated, well-maintained infrastructure were more resistant to cyberattacks. However, the study emphasised that owning technological infrastructure alone was insufficient; competent staff, frequent updates, and continuous maintenance were all required. Cheng and Li (2020), who found that the use of cloud computing significantly improved data security and recovery times after cyberattacks by police forces. However, the researchers discovered potential weaknesses associated with cloud computing, such as dependence on outside service providers and worries about data breaches. In a different context, Anderson and Kumar (2021) agree with Cheng and Li (2020) that technology enhanced data collection capabilities and operational efficiency, but it also introduced new vulnerabilities that hackers could exploit.

2.3 The influence of human resource capabilities on cybersecurity resilience

Mizrak (2023) asserts that the understanding that employees are both possible assets and liabilities in an organization's cyber defence strategy forms the basis of the relationship between cybersecurity and human resource capabilities (HRC). The Human Resources Committee has traditionally been in charge of hiring, training, managing staff, and creating a positive work environment. Businesses now understand the human component of cybersecurity and are investigating the relationship between HRM practices and the overarching objective of bolstering their cyber defences. The connection is complex and involves hiring procedures, awareness-raising initiatives, employee education, and the creation of an organisational culture that places a high priority on cybersecurity. Understanding this complex relationship is essential for using HRC as a strategic resource in cybersecurity risk management (Llorens, 2017).

The development and execution of successful employee awareness and training initiatives depend heavily on human resource capabilities. Thorough cybersecurity training gives employees the knowledge and abilities they need to identify potential threats and take

appropriate action. This proactive approach reduces the likelihood of falling victim to social engineering tactics like phishing by empowering employees to act as the first line of defence against cyber threats. Continuous awareness campaigns highlight the importance of security procedures in day-to-day operations and foster a culture sensitive to cybersecurity (Menaka, 2022). Including security awareness in the hiring process is one way to strategically incorporate cybersecurity considerations into HR practices. A workforce with a security-focused mindset may be promoted by putting in place thorough background checks and testing people's cybersecurity knowledge. Potential insider threats can be reduced by this proactive screening, which also makes sure that those in important positions align with the cybersecurity goals (Singh & Sharma, 2020).

Human resources and information technology departments can work together to set up privilege management and role-based access controls. By aligning access permits with job responsibilities, Human Resource Capabilities ensures that workers have the necessary access rights free from unnecessary privileges. This lessens the possibility of illegal access to private data and the possible repercussions of insider threats. When Human Resource Management is involved in the creation and implementation of access controls, the organisational structure's security is improved (Gillam, 2019). In addition to specific programs and initiatives, HRC can support the development of an organisational culture focused on cybersecurity. This means encouraging staff members at all levels to take responsibility for cybersecurity. Through efficient communication, policy enforcement, and support, HRC may create an environment where cybersecurity is viewed as a shared responsibility rather than just an IT problem (Madaan et al., 2023). Together with the IT and cybersecurity departments, the HRC can create and implement incident response training initiatives. By clearly defining roles and responsibilities, the HRC ensures that members are sufficiently equipped to react quickly and effectively to cybersecurity incidents. This includes communication protocols, crisis management training, and cooperation with outside parties. Overall defence against cyberthreats is strengthened by these proactive measures (Kalia & Mishra, 2023).

Integrating security awareness into the hiring process is one way to strategically integrate cybersecurity considerations into HR practices. A workforce with a security-focused mindset can

be developed by putting thorough background checks into place and testing people's cybersecurity knowledge. Potential insider threats can be reduced by this proactive screening, which also makes sure that those in important positions align with the company's cybersecurity goals (Singh & Sharma, 2020). To create role-based access controls and privilege management systems, the HR Committee can collaborate with IT departments. HRC ensures that workers have the necessary access rights free of unnecessary privileges by aligning access permissions with work responsibilities. This lessens the chance of unauthorised access to private data and the potential impact of insider threats. By creating and managing access controls, the Human Resources Committee improves the organisational framework's security (Gillam, 2019).

Human Resource Capabilities can help create a culture of cybersecurity in the workplace through certain programs and activities. This means that everyone in the organisation needs to feel responsible for cybersecurity. HRC can create an environment where everyone in the organisation sees cybersecurity as a shared responsibility, not just an IT issue, by communicating well, enforcing policies, and providing organisational support (Madaan et al., 2023). The HRC can work with the IT and cybersecurity departments to make and carry out training programs for responding to incidents. HRC makes sure that employees are ready to respond quickly and effectively to a cybersecurity event by clearly outlining their roles and responsibilities. This includes how to talk to people, how to handle crises, and how to work with people outside the company. These proactive steps make the organisation more resistant to cyber threats overall (Kalia & Mishra, 2023).

There have been a number of studies that looked at the link between police operations' cybersecurity resilience and the skills of their human resources. Some of the most important were: Smith and Rahman (2022) wanted to find out if there was a link between improving the skills of law enforcement officers and being ready for cyberattacks. The study found that spending money on people, especially on ongoing education and skill development, is strongly linked to higher levels of cybersecurity readiness.
Nash and Yavuz (2019) wanted to find out how good law enforcement agencies' human resources were at cybersecurity, focussing on what skills they were missing and what training they needed. The study found that law enforcement officials are very bad at cybersecurity,

especially when it comes to identifying advanced threats and responding to incidents. The study showed that basic cybersecurity training was common, but there was a lack of advanced skills. Turner and Morris (2020) looked into how human resource capabilities can help police organisations become more resilient to cyberattacks. The study found that human resource capabilities like targeted hiring, ongoing professional development, and performance monitoring are necessary for making cybersecurity more resilient. Still, differences in how departments handle HRM were seen as a barrier to achieving consistent cybersecurity resilience.

2.4 Conformity of cybersecurity resilience practices with international norms.

Murphy and Yates claim that studying standard-setting organisations that primarily function behind closed doors but carry out tasks that governments support and have a big impact on day-to-day life can provide important insights into global governance (Murphy and Yates 2009, 12). According to the authors, standard-setting organisations have taken on an informal role in establishing norms, especially through the development of technical standards pertaining to Cybersecurity matters, as a result of states' difficulties reaching a formal consensus on complex issues through transnational policy-making.

The absence of agreement on practices has led to almost legal, or "soft-law," as shown by the way they are often used in relation to laws. People often call the role of standards in filling in legal gaps and helping to meet policy goals a "para-legal function" (Senden and Brink 2012). Löhe and Blind say that standards created in line with regional laws, like ISO/IEC 27018, which deals with how personal data is handled in cloud computing, could make the substantive provisions of those laws apply to more places than just where they were made (Löhe and Blind 2015). In this case, one could say that the use of the international standard serves a quasi-legal purpose in countries that don't have rules for cloud computing. Governments that choose to use European harmonised standards can assume that they are following the law (Joerges, Schepel, and Vos 1999). The designated state leaders set the basic requirements, and the technical committee in charge of creating the standard decides exactly how those requirements are spelt out in the controls and rules of the harmonised standard.

The European Commission, for instance, often uses the term "cyber resilience" to refer to keeping networks safe from bad attacks. In its 2013 Cybersecurity Strategy for the European Union, the European Commission said that making the EU more cyber-resilient was its top goal. It did this by, among other things, getting public and private organisations to work together better and making sure that its states had better cybersecurity skills in both sectors (European Commission 2013). The Network and Information Security Directive (NIS Directive) was the first law proposal from the European Union to improve cyber resilience. It came with the Cybersecurity Strategy. Its goals were to "improve the preparedness and engagement of the private sector," set up "coordinated prevention, detection, mitigation, and response mechanisms," and set "common minimum requirements for network and information security" (European Commission 2013, 5). The 2013 NIS Directive made the idea of cyber resilience a reality by making it a legal requirement.

In 2013, fifteen countries, including the United States and China, agreed that international law, in particular, the United Nations Charter applies in cyberspace and explicitly highlighted the need to elaborate confidence-building measures and norms, rules, or principles of responsible behavior of states (UN General Assembly Report 2013). UN member states have contributed in varying degrees to requests by the General Assembly to report on their views on international law and cooperation to prevent destabilization of state relations in cyberspace. According to a recent study by the UN Institute for Disarmament Research, more than 40 states have now developed some military cyber capabilities, 12 of them for offensive cyber warfare (UN Institute for Disarmament Research 2013).

Fifteen countries, including the US and China, agreed in 2013 that international law, especially the UN Charter, applies to the internet. They also stressed how important it is for states to follow norms, rules, or principles of responsible behaviour (UN General Assembly Report 2013). The General Assembly has asked all UN member states to tell them what they think about international law and working together to keep state relations stable in cyberspace. Some countries have done this more than others. The UN Institute for Disarmament Research recently

found that more than 40 countries already have some military cyber capabilities, and 12 of them are for offensive cyber warfare (UN Institute for Disarmament Research 2013).

The Charter of the United Nations, which almost all countries have signed, sets rules for how the organisation works and how countries should act (UN 1945). However, different governments may have different ideas about how to carry out the UN's goals and objectives. The NATO Cybersecurity framework manual says that National Cybersecurity has five main areas of responsibility: (1) Military Cyber, (2) Counter Cybercrime, (3) Intelligence and Counter-Intelligence, (4) Critical Infrastructure Protection and National Crisis Management, and (5) Cyber Diplomacy and Internet Governance. It also has three cross-mandates: coordination, information exchange and data protection, and research, development, and education (Klimburg 2012). Even though the United Nations Charter and NATO's Cybersecurity architecture say otherwise, there is no perfect cybersecurity model that works for all governments.

The discussion about governance and cooperation in Africa for security and stability in cyberspace has been largely unexplored (Microsoft 2021). There are a lot of questions about how well African governments can protect the region from cyber threats because Africa isn't ready for cyber governance (Schlehahn 2020). There are also worries about how well African countries can regulate cyberspace with laws that meet international standards. Because their digital skills and political systems are so different, African countries also seem to have a hard time following the rules for how states should act in cyberspace. People are also worried about how African leaders feel about and deal with digital sovereignty. They are also worried that working together online could mean relying on other people digitally when their digital skills are different.

2.5 Research Gaps

There isn't much empirical evidence on cybersecurity resilience in Africa, mostly because modern technologies like surveillance systems, biometric systems, and digital number plates are slow to catch on. People don't often look into how Africa's outdated or inadequate infrastructure affects cyber threat detection, response, and recovery. There aren't enough models that show how infrastructure maturity (like bandwidth, secure networks, and cloud use) affects real-world

resilience outcomes in police settings. Not enough study has been done on how hard it is to combine traditional policing tools with new ICT-based methods in Africa. This further characterized by the lack of research on how often infrastructure failures or human resource capabilities in Africa have increased cybercrimes.

CHAPTER THREE

PRESENTATION OF FINDINGS

3.1. The effect of technological infrastructural development on cybersecurity resilience in the Ugandan Police Force.

Crimes such as cyber terrorism, intellectual property infringement, internet usage policy abuses, internet fraud, industrial espionage and altering of data, on-line child exploitation and pornography, illegal goods purchasing, piracy, impersonation and hacking" still exist in Uganda (Mulalira, n.d.). For example, in 2005, a Ugandan and two Congolese masterminded the internet bank transfer of a massive sum of money from Standard Charted Dank, Nairobi to Barclays Bank, Kampala (Tushabe, 2004). Similar crimes have been committed against other banks such as the Centenary Bank. Collectively, banks in Uganda have lost billions of Ugandan Shillings due to cybercrime. The amplification of cybercriminal activity can be credited to many companies operating with inadequate funding and financial capabilities in fighting cybercrime.

Alungat (2023) says that crime has changed as technology has gotten better, and criminals are now using technology to make Kampala metropolitan unsafe and less peaceful. Some examples of crimes are drug trafficking, bank fraud, cybercrime, terrorism, murder for love or money, and smuggling. The Uganda police has been training its staff to become experts in new cyber technology since 2010 so that they can stay one step ahead of suspected criminals in cyber crimes. Today, photographers from the Uganda Police can send digital photos of crime scenes to the forensic lab for analysis instantly from the crime scenes. This also includes tracking and use of videos from CCTV cameras that are now all over Kampala and most urban areas in Uganda.

Some streets in Kampala and Entebbe had CCTV cameras on them in 2007 to keep an eye as Uganda got ready to host CHOGM. This was done to make the important routes and junctions safer for the delegates who were coming. There were, however, more terrible murders in the Kampala metropolitan area. Because of this, the president of Uganda gave the go-ahead for Closed-Circuit Television (CCTV) cameras to be put up along major highways, towns, and cities all over the country to help lower crime. The first phase of installation took place in the Kampala Metropolitan policing area, where 3,233 cameras were put up (Annual Crime Report 2020). CCTV cameras started going up in Kampala in July 2018. The goal of putting up CCTV cameras was to help the Uganda Police and other security groups stop crime from getting worse in the country. The police watch the CCTV cameras that have also been helpful in fighting cybercrimes.

There are three main ways in which cybersecurity issues are classified in Uganda. The risks to technology security, the threats of cybercrime and espionage, and the threats to military civil defence. There are cybersecurity problems in Uganda at the individual, state, and international levels. When people don't have good personal security measures in place and don't know how to keep their computers and electronics safe, they are more likely to be exposed to risks and vulnerabilities. At the state level, this is shown by problems with communication caused by criminal groups operating within national borders, cyber attacks for financial gain, and other things. Espionage aimed at getting information on different groups, especially government ministries, departments, and agencies, as well as hostile actors doing counter-propaganda operations against the state, create external threats. Governments and other outside groups use Distributed Denial of Service Attacks (DDoS) and malware to cause widespread problems. In the digital age, military-civil defence threats, also known as information warfare targeting key infrastructures, are very common. The Uganda Police cybercrime unit and the Uganda People's Defence Forces cyber defence units are examples of organisations in Uganda that deal with these issues.[5]

Technical cyber security problems happen when hackers still mostly go after computers and computer networks. It has to do with malware, which is a type of software that includes viruses,

[5] M, Owiny (2023). Assessing Institutional and Cybersecurity Capacity in Uganda. Centre for Multi-Lateral Affairs. https://thecfma.org/2023/02/15/assessing-institutional-and-cybersecurity-capacity-in-uganda/

worms, Trojans, and system intrusions. The fact that computer malware is so common has long been clear proof of how unsafe the information infrastructure is. The Uganda Police Crime Report of 2022 says that the rise in cybercrime, which was 10.8%, caused losses of UGX 19.2 billion. This is very worrying. Part of the reason for this is that the Ugandan police haven't bought the newest tools they need to keep up with what cyber criminals need. Cybercrime in Uganda has grown from a few isolated cases to a lot of attacks on businesses in recent years. MTN Uganda, the country's largest telecommunications company, was the victim of a scam that cost the company and the government millions of Ugandan Shillings (Ndagire, 2020).

On November 17, 2023, the Observer Newspaper stated that Museveni had mandated the prompt adoption of digital license plates. The digital car registration plate initiative has been formally launched by the Ugandan government through the ministries of Works, Transport, and Security. In order to install digital tracking chips in all registered vehicle number plates nationwide, the government has launched the Intelligent Transport Management Systems (ITMS) program, which will take ten years. Enhancing security, which includes tracking down cybercriminals, is the aim. According to Uganda's president, installing license plates will lower crime as follows;

"I'm now insisting on the electronic number plates. Please, I want my number plates. Don't delay my number plates. I don't want these aimless number plates. I want intelligent number plates for the vehicles. The electronic number plates will significantly help in investigations of crimes now that the force is using all the comprehensive means and assets needed for the job".

HE Yoweri Kaguta Museveni, the President of Republic of Uganda

The above excerpt from the President shows the likely effect of digital infrastructure in reducing crime in Uganda as the new number plates will be used to track cyber criminals in real time after identification by CCTV cameras in the urban centres. The development of an integrated technological system is a good step for the Ugandan police to general deal with crime in the Kampala Metropolitan area.

3.2. The influence of human resource capabilities on cybersecurity resilience in the Ugandan Police Force

The Uganda Police Force is a government entity closely connected to the community, tasked with maintaining peace and security in urban areas. Its principal function is to constitutionally

protect individuals and their property. Nevertheless, the swiftly proliferating urban environments influenced by technology are presenting escalating obstacles for law enforcement and raising concerns regarding the capacity of the Ugandan police to ensure security. In 2014, the ICT Directorate of the Uganda Police Force finalised a significant enhancement of the 999 emergency service line. This was intentionally reinstated for public use in the event of any imminent threat to life and public safety, as well as in circumstances necessitating an expedient reaction.

The emergency contact centre accepts calls and subsequently alerts the motorised response team to act. The 2020 Annual Crime Report said that by 2021, the Motorised 999 system had 18 motor vehicles allocated throughout all Divisions in the Kampala Metropolitan Area. This facilitates the closure of gaps by performing patrols in areas without CCTV surveillance. As a result, they prevented multiple robberies by swiftly addressing calls, including those concerning cybercrimes. On April 23, 2022, in reaction to public concern over the increase in cyber-crime committed by fraudsters, the Territorial Police of Nansana executed an intelligence-led operation in the Nansana West 2A Kibulooka region aimed at organised criminal syndicates engaged in electronic fraud and offensive communication.

The Ugandan police in coordination with sister security agencies such as the UPDF, Prisons, SFC, JIC (CMI, ISO, CI, and ESO), JATT, combated various forms of crime including cyber crimes. The police with other security agencies attend courses at Senior Command and Staff College Bwebajja which has improved working relations among them. These joint initiatives have resulted in the reduction of cybercrimes such as online fraudsters with in the Kampala Metropolitan area. Cyber security resilience in police has therefore been achieved through the hard work of the police in coordination with sister security agencies, the reorganisation of the CID (Criminal Investigations Directorate), improved detection and investigation methods, and the establishment of a proactive network of credible intelligence. Furthermore, Police in Kampala has created a strategic partnership with the community, including the involvement of other intelligence components that have greatly contributed to disrupting and dismantling criminal elements(Annual crime report, 2023).

Interagency collaboration and coordination have consequently enhanced the Uganda Police Force's capacity to fortify urban security overall. The Uganda Police Force now engages in

interagency cooperation and coordination with other security agencies for training, operations, events, celebrations, and the establishment of joint command centres. This facilitates capacity growth through information exchange and resource mobilisation, including persons with specialised technical capabilities. Interagency cooperation and collaboration unite security and public safety agencies to operate across organisational and jurisdictional boundaries, facilitating response and administrative functions. This alliance benefits citizens through coordinated deployment, complementary skills, improved financial resource utilisation, and enhanced public perception of emergency services (Sheridan, 2019). The cooperation can be implemented through bilateral or multilateral collaboration, joint task forces, memoranda of understanding, statutory organisational assets and strengths, as well as ad hoc and case-by-case arrangements utilising networks of informal lawful personal contacts at strategic, operational, and tactical levels for threat assessment, disruptive, and preventive interventions against crime; however, issues of command and resources must be regularly evaluated (Chukkol, 2019).

Local leaders, political leaders, Resident District Commissioners/Resident City Commissioners, the Uganda Police Force, and the judiciary are all important to the cyber security of the Kampala Metropolitan region. The District Security Committee (DSC) is very important in a district for planning and coordinating the implementation of peace and security measures. The DSCs are like the National Security Committee, where important decisions and policies for keeping cities safe and peaceful are made, carried out, and reviewed (Alungat, 2023). These include early warning systems and disaster management. The military, intelligence agencies, and police work closely in the fight against cybercrimes. All these efforts mentioned to coordinate security have become an important part of the skills needed in the Kampala Metropolitan area to make cybersecurity more resilient.

To enhance urban peace enforcement in the Kampala Metropolitan area, Ugandan police have made a great effort to implement an intelligence-led policing strategy. It is common for criminals to be involved in cybercrimes in Kampala, a city with a large population and numerous slums. Intelligence-led policing, according to Tilley (2003), is a style of policing that concentrates on obtaining copious amounts of information about criminal activity so that patrols and law enforcement can concentrate on preventing crime. According to him, intelligence policing is a collaborative process that starts with information gathering, such as the locations of crimes and

the resources available to create intelligence that could help analyse and assess ongoing operations. It aims to make choices that will enable people to make informed decisions regarding tactics, resource allocation, and tactical action execution. According to the Director of Operations in the Ugandan Police Force, Grace Turyagumanawe, argues that intelligence will be in the lead, backed up by other agencies in the coalition activities to fight crime. He further connotes that police today emphasize the need for popular intelligence to ensure security agencies work with the population, LCs and crime preventers as a way to reduce crime[6].

3.3. Conformity of cybersecurity resilience practices with international norms by the Uganda police

The Ugandan government has armed itself with a number of laws that ensure the security of the cyberspace because cybercrimes directly affect people when they lose important data, have their money stolen, or have their privacy violated. Underpinned by earlier laws like The Official Secrets Act, 1964 (Section 4(1)(d)) and The Security Organisations Act, 2005, the Ugandan government created and passed a number of cyber laws in an attempt to provide a suitable legal framework to deal with cybercrime and provide for secure electronic transactions. These laws include The Computer Misuse Act, 2011, The Electronic Signatures Act, 2011, and The Electronic Transactions Act, 2011. To ensure a strong readiness in cyberspace security, the Ugandan government has also established the National Information Security Strategy (NISS), 2011, the National Information Security Framework (N1SF), and the Communications Sector Computer Emergency Response Team (CERT) (ict.go.ug).

The Computer Misuse Act, 2011, The Electronic Signatures Act, 2011, The Electronic Transactions Act, 2011, The Electronic Misuse Act, The Access to Information Act, 2005, and The Regulation of Interception of Communications Act, 2010 (GCSCC, OMS, UO, & CTO, 2016: 14) all are being used by the Uganda police to keep the country safe online. Uganda's law enforcement agencies don't have the time or money to look into every crime, but these legal tools have helped the country's cyber security enforcers to bring offenders to book. The Cyber Crime

[6]Malaba, T(2013). Police Invests In Intelligence To Fight Crime. Uganda Radio Network. https://ugandaradionetwork.net/story/police-invests-in-intelligence-to-fight-crime?districtId=505

Unit and Electronic and Counter Measures Department of the Uganda Police Force usually have the technical skills and training to find criminals and build cases against them. But some of the laws that police use, like the CMA, don't say what cybercrime is. Many different ideas existed about what actions fall under cybercrimes before the CMA was passed. It would have made sense to expect that these kinds of laws would at least have a clear definition of what cybercrime is. The CMA which is the most commonly used law by police doesn't clearly define cybercrime, so it's hard to know what this term really means.

Governments have created and passed many laws to combat cybercrime because it occurs all over the world. In a report titled "Understanding cybercrime: phenomena, challenges and legal response," published by the International Telecommunication Union, Gercke (2012) discussed a number of these international legal frameworks for combating cybercrime. He argues that member states are required to prohibit the abusive exploitation of children in pornographic performances under Article 34 of the United Nations Convention on the Rights of Children (UNCRC). Article 3 of the Optional Protocol on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography mandates that State parties outlaw certain behaviours, including those associated with child pornography (Gercke, 2012: 116). Uganda is a party to the United Nations Convention on the Rights of the Child (UNCRC). It ratified the convention in 1990. This shows that Uganda has committed to upholding children's rights as outlined in the UNCRC. The two Optional Protocols on the sale of children, child prostitution and pornography, and the participation of children in armed conflict were also signed by Uganda. This demonstrates the nation's commitment to upholding the rights of children.

Article 3(l)(c) of the Optional Protocol to the Convention on the Rights of the Child (2001) says that it is against the law to make, share, sell, or own child pornography. The Preamble says that the Internet can be used to get the word out. Article 2(3) gives a wide definition of child pornography that includes pictures of kids that are not real (2171 U.N.T.S. 227). Article 21 (1)(f) of the European Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) says that "information and computer technology (ICT)" can't be used to get child pornography, share it (Article 30(5)), or ask kids for sexual favours (Article 23) (C.E.T.S. 201). On June 22, 2022, the Territorial Police in Kabalagala, which is part of the Kampala metropolitan area, arrested a cybercriminal who ran a website for sex and porn. According to

intelligence reports, she rented an apartment where she lured young girls and showed their naked bodies online in exchange for money.[7]

Uganda is currently at crossroads in terms of international cyber governance because the rules don't always fit with the problems it has with its people and infrastructure. Most African countries that have a digital gap don't have the funds, knowledge, or infrastructure to properly enforce cyber governance at international standards (Calandro, 2021). Castells says that Africa's ICT infrastructure isn't as good as it should be by today's standards(Castells 2001). He said that the gap between people who have ICT and those who don't is big. So, places like Uganda can't possibly be part of talks about international cyber governance at the same wave length.

The Malabo Convention was meant to help African countries like Uganda make rules and set an example for cyber security laws, but it also has a lot of problems (Zahid 2016). The structure of the Malabo Convention: it will be hard to combine cybersecurity and data protection, especially since the Convention's data protection rules don't say anything about cybersecurity. The definitions in the Malabo Convention aren't as detailed as those in other related documents, like the Budapest Convention. It might also be hard to believe for some countries like Uganda that the Malabo and Budapest Conventions are rivals and have different goals. African countries need to know that model laws and agreements like the Budapest agreements are not a replacement for the Malabo Convention; they are only meant to add to it. One reason the Ugandan government is taking so long to ratify the Malabo and Budapest conventions is that they limit the laws that the Ugandan police have to follow to keep data, cyber security, and electronic transactions safe. It is hard to trust Uganda's cyber rules in the international system because they haven't ratified to these two main treaties. This makes it harder for countries to work together with Uganda in terms of cooperation and collaboration on cyber security.

Because of this, Uganda's legal and institutional framework does not meet international standards. The Ugandan government has admitted that its laws about what happens in the cyberspace industry and cybercrimes are not very strong. One reason is that the laws that are meant to stop cybercrimes are still new, so they aren't being enforced very well. As internet technology gets better, new crimes that aren't covered by the law make it harder to enforce

[7] Uganda Police(2022). Police busts on line sex and pornography hub. https://upf.go.ug/police-busts-on-line-sex-and-pornography-hub/

cybercrime laws. This means that the current laws in Uganda that are supposed to stop cybercrime might not be enough to deal with these new and changing types of crime. Based on what we've talked about, this could help explain why cybercrime rates in Uganda have gone up (Adesuyi, 2020).

CHAPTER FOUR

CONCLUSION AND RECOMMENDATIONS

4.1 Conclusion.

As technology has improved, so has crime. Now, criminals use technology to make the Kampala metropolitan area less safe and peaceful. Drug trafficking, child pornography, bank fraud, cybercrime, terrorism, murder for money or love, and smuggling are all examples of crimes. Since 2010, the Uganda police have been training their officers to use new cyber technologies so they can stay ahead of people they think are cybercriminals.

These days, Uganda Police photographers are able to send digital photos of crime scenes straight from the scene of the incidents to the forensic lab for examination. This includes keeping an eye on and using CCTV footage, which is becoming more and more common in Kampala and most Ugandan cities.

The ministries of Works, Transport, and Security have officially started the digital car registration plate program in Uganda. The government has started the Intelligent Transport Management Systems (ITMS) program, which will take ten years to put digital tracking chips in all registered vehicle number plates across the country. Adding to these security measures makes it easier to find cybercriminals.

The Uganda Police Force is a government agency that works with the people to keep cities safe and peaceful. The law says that its main job is to protect people and their property. The Uganda Police Force's ICT Directorate finished a big upgrade to the 999 emergency service line in 2014. The Motorised 999 system had 18 motor vehicles allocated throughout all Divisions in the Kampala Metropolitan Area. This facilitates the closure of gaps by performing patrols in areas without CCTV surveillance.

The Ugandan police worked with other security services, such as the UPDF and Prisons. These groups working together have helped lower cybercrimes in the Kampala Metropolitan area, like fraud online. Sharing information and getting people with specialized technical skills to work together helps build capacity.

The Ugandan police have worked hard to put in place an intelligence-led policing policy in the Kampala Metropolitan region to make it easier to keep the peace in cities. It aims to help people make smart choices about tactics, how to use resources, and how to carry out tactical actions. The Uganda police stress the importance of community intelligence today in order to help security services, local councils, and crime preventers work together to reduce crime.

Because cybercrimes directly affect people by causing them to lose important data, have their money stolen, or have their privacy violated, the Ugandan government has passed a number of laws to protect cyberspace. To create a suitable legal framework for combating cybercrime and guaranteeing secure online transactions, the Ugandan government created and passed a number of cyber laws. The laws include the Electronic Transactions Act of 2011, the Computer Misuse Act of 2011, and the Electronic Signatures Act of 2011.The Ugandan government has put in place the National Information Security Strategy (NISS) of 2011, the National Information Security Framework (N1SF), and the Communications Sector Computer Emergency Response Team (CERT) to make sure they are ready for cyber security threats.

Uganda is a signatory to the United Nations Convention on the Rights of the Child (UNCRC). It ratified the convention in 1990. This indicates that Uganda is dedicated to safeguarding children's rights as specified in the UNCRC. Uganda also signed the two Optional Protocols concerning the sale of minors, child prostitution and pornography, and the involvement of children in armed conflict. This exemplifies the nation's dedication to safeguarding children's rights.

Uganda presently faces a dilemma in international cyber governance, as existing regulations often do not align with the challenges posed by its populace and infrastructure. Similar to many African nations, those with a digital divide lack the financial resources, expertise, or infrastructure necessary to implement cyber governance in accordance with international norms.

Trust in Uganda's cyber regulations within the international framework is compromised due to their failure to ratify the essential treaty on cybercrime. This complicates international cooperation and collaboration on cybersecurity with Uganda. Consequently, Uganda's legislative and institutional framework fails to align with international standards. The Ugandan government has acknowledged that its cyber security legislation is inadequate and poorly enforced.

4.2 Recommendations.

The government must augment financing for the Ugandan police to acquire advanced cyber-crime management technology to combat the sophisticated criminals attacking commercial banks and mobile money centers in the Kampala Metropolitan area.

The government should implement a comprehensive Human Resource structure that delineates cybersecurity jobs, requisite competences, recruiting criteria, and career advancement pathways within the Uganda Police Force. The government must invest in security partnerships, beginning with enhanced joint training and skill development initiatives in cybersecurity to strengthen capabilities against cyber threats in Uganda. This also encompasses enhancing community policing and intelligence gathering systems to bolster early warning mechanisms in the city center.

Uganda ought to ratify all essential conventions on cybersecurity to foster collaborations and international cooperation with developed nations that may offer advanced technology and training to law enforcement for the detection, apprehension, and mitigation of emerging cybercrimes within the country.

References.

Chen, L., & Wang, Z. H. (2018). A Study on the Status Quo of Chinese College Students' Intercultural Communication Competence. Chinese Studies, 7, 164-173. https://doi.org/10.4236/chnstd.2018.72014.

International Telecommunication Union (ITU). (2022). Global cybersecurity index 2022**.** https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Anderson, T. (2008). The Theory and Practice of Online Learning. Athabasca University Press.

Ajayi, J. (2023) 'Fake News on Steroids: The Urgent Need for Nigeria to Regulate Artificial Intelligence'. 15 December www.linkedin.com/pulse/fake-news-steroids-urgent-need-nigeriaregulate-artificial-john-ajayi-nnnke/

IBM (nd) 'What Is Cyber Resilience?' www.ibm.com/topics/cyber-resilience (accessed 25 November 2024).

Sibe, R. (2024) 'Cybercrime and the Challenge of Static Legislations in Nigeria'. Forbes, 29 April. www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-ofstatic-legislations-in-nigeria/

Rogers, P. (2020) 'The Evolution of Resilience'. Connections Quarterly Journal 19(3): 13–32.

Smith, S. (2023) 'Towards a Scientific Definition of Cyber Resilience'. Proceedings of the 18th International Conference on Cyber Warfare and Security.

Araujo, M., Machado, B. and Passos, F. (2024) 'Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance'. Applied Sciences, 14. https://doi.org/10.3390/ app14052116

AL-Hawamleh, A. (2024) ‘Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security’. International Journal of Computing and Digital Systems 15(1): 1315–1331.

Nwafor, I, Nwafor, N. and Alozie, J. (2021) ‘Revenge Pornography in Nigeria: A Call for Legal Response and Cyber-Censorship of Content by Internet Service Providers’. African Journal of Legal Studies 13(2): 1-27.

Ross, R., Pillitteri, V., Graubart, R. et al. (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2, Rev. 1. https://csrc.nist.gov/pubs/ sp/800/160/v2/r1/final

Mugisha, P., & Namanya, C. (2020). Technological infrastructure and cybersecurity resilience in the Ugandan police force. *Journal of Information Security in Africa*, 11(4), 112-127.

Katureebe, J. (2022). Human resource capabilities and cybersecurity resilience in the Ugandan police force. *Uganda Journal of Law and Technology*, 14(1), 34-51.

Mbabazi, E. (2023). Inter-agency collaboration and cybersecurity resilience in Uganda: Challenges and prospects. *East African Security Review*, 19(1), 45-62.

Uganda Police Force. (2019). Annual crime report 2019**.** https://www.upf.go.ug/annual- crime-report-2019/

Hollnagel, E., Woods, D.D. & Leveson, N. (2006). Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd., Aldershot, UK.

Chigudu, A., & Chavunduka, C. (2021). The Tale of Two Capital Cities: The Effects of Urbanisation and Spatial Planning Heritage in Zimbabwe and Zambia. *Urban Forum, 32*, 33-47. https://doi.org/10.1007/s12132-020-09410-8

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44, 588-608. http://dx.doi.org/10.2307/2094589

Messner, S. F. and K. Tardiff. 1985. "The social ecology of urban homicide: A application of the routine activities approach." Criminology 23: 241-267.

Cohen, L. E. and M. Felson. 1979. "Social change and crime rate trends: A routine activity approach." American Sociological Review A4'. 588-608.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25. https://doi.org/10.1080/01639620701876577

van Wilsem, J. A. (2011). 'Bought it, but never got it'. Assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168–178. https://doi.org/ 10.1093/esr/jcr053

Bossler, A., Holt, T. J., & May, D. (2012). Predicting online harassment: Victimization among a juvenile population. Youth & Society, 44(4), 500-523. https://doi.org/10.1177/0044118X11407525

Choi, K-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2(1), 308-333.

Michael Fischerkeller, Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage (Institute for Defense Analyses: Alexandria, VA, 2018), p. 15, fn 58. Fischerkeller refers to low barrier to entry as an operational incentive for operational persistence vice a strategic imperative.

Cullen, KA., Ambrose, BK., Gentzke, AS., Apelberg, BJ., Jamal, A., & King, BA. (2018). Notes from the field: Use of electronic cigarettes any tobacco products among middle and high school students – United States, 2011-2018. Morbidity and Mortality Weekly Report. 67, 1276-1277. https://doi.org/10.15585/mmwr.mm6745a5

Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J., Brummel, B.J., 2022. Organizational science and cybersecurity: abundant opportunities for research at the interface. J. Bus. Psychol. 37, 1–29.

Niemimaa, M. (2023). Evaluating compliance for organisational information security and business continuity: Three strata of ventriloqual agency. Information Technology & People (ahead-of-print). https://doi.org/10.1108/ITP-03-2022-0156

Cedergren, A., Johansson, J., & Hassel, H. (2018). Challenges to critical infrastructure resilience in an institutionally fragmented setting. Safety Science, 110, 51–58. https://doi.org/10.1016/J.SSCI.2017. 1

Iryna Leroy & Iryna Zolotaryova & Serhii Semenov, 2025. "**Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors**," Sustainability, MDPI, vol. 17(3), pages 1-21, February

Akter, S., Gunasekaran, A., Wamba, S.F., Babu, M.M., Hani, U., 2020. Reshaping competitive advantages with analytics capabilities in service systems. Technol. Forecast. Soc. Chang. 159, 120180.

Singh, Gurmeet & Sharma, Shavneet, 2020. "**Modelling internet banking adoption in Fiji: A developing country perspective**," International Journal of Information Management, Elsevier, vol. 53(C).

Paper, Craig Murphy and JoAnne Yates, "ISO 26000: Fulfilling the Social Promise of Voluntary Consensus Standard Setting? Part I," presented by Craig Murphy at the ABRI-ISA Joint Convention, Rio de Janeiro, July 22-24, 2009 www.allacademic.com/meta/p_mla_apa_research_citation/3/8/1/1/3/p381135_index.html. Paper,

Craig Murphy and JoAnne Yates, "Re-Embedding Global Capitalism through Voluntary Standards: Can ISO 26000 Fulfilling the Historical Promise of Voluntary Consensus Standard Setting?" presented by Craig Murphy at the University of Southern California, Center for International Studies, October 21, 2009.

Senden, Linda and Anton van den Brink (2012). Checks and Balances of Soft EU Rule-Making'. Study conducted for Policy Department C: Citizens' Rights and Constitutional Affairs. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042480 [accessed 18 June 2020].

National Information Technology Authority, Uganda (NITA-U). (2021). National Information Security Framework (NISF)**.** https://www.nita.go.ug/publication/national-information-security-framework-nisf

National Strategy to Secure Cyberspace. (2003). *The White House*.

Leukfeldt E R and Yar M 2016 Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis Deviant Behavior 37 263–80

Kigerl A 2012 Routine Activity Theory and the Determinants of High CybercrimeCountries Social Science Computer Review 470–86

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801–814. https://doi.org/10.1080/13669877.2023.2208146

Sawyer, S., and M. H. Jarrahi. 2014. "Sociotechnical Approaches to the Study of Information Systems." Chapter 5 in *Computing Handbook: Information Systems and Information Technology*, eds. H. Topi, and A. Tucker, 3rd Ed. New York: Chapman and Hall/CRC. doi:10.1201/b16768.

Interpol. (2020). Interpol cybercrime strategy 2020-2023**.** https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-strategy-2020-2023

Nash, M. & Yavuz, K. (2019). Human resources and cybersecurity in law enforcement: assessing capabilities. *Journal of Law Enforcement Technology*, 12(2), 145-162. doi 10.1177/1948550619900311

O'Brien, M., & Jenkins, S. (2018). The role of cybersecurity infrastructure in police resilience: A mixed-methods analysis. *International Journal of Police Science & Management*, 20(4), 275-290.

Government of Uganda. (2011). The Computer Misuse Act (2011)**.** https://www.nita.go.ug/sites/default/files/publications/Computer%20Misuse%20Act%202011.pdf

Haddad, C., & Binder, C. (2019). *Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society. Österreichische Zeitschrift Für Soziologie*, 44(S1), 115–134. doi:10.1007/s11614- 019- 00350-7

Schlehahn, E. 2020. "Cybersecurity and the State." In *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology*, edited by M. Christen, B. Gordijn, M. Loi. Switzerland: Springer.

Joerges, Christian, Harm Schepel & Ellen Vos (1999) 'Delegation' and the European Polity: The Law's Problems with the Role of Standardisation Organisations in European Legislation, EUI Working Paper in Law 9-1999, http://www.iue.it /LAW/WP-Texts/law99-9.pdf

Madaan, A.; Tandon, N.; Gupta, P.; Hallinan, S.; Gao, L.; Wiegreffe, S.; Alon, U.; Dziri, N.; Prabhumoye, S.; Yang, Y.; Welleck, S.; Majumder, B. P.; Gupta, S.; Yazdanbakhsh, A.; and Clark, P. 2023. Self-Refne: Iterative Refnement with Self-Feedback. CoRR.

Slack, N., Singh, G., & Sharma, S. (2020). The Effect of Supermarket Service Quality Dimensions and Customer Satisfaction on Customer Loyalty and Disloyalty Dimensions. International Journal of Quality and Service Sciences, 12, 297-318. https://doi.org/10.1108/IJQSS-10-2019-0114,

Llorens, M. G., Griera, A., Steinbach, F., Bons, P. D., Gomez-Rivas, E., Jansen, D., Roessiger, J., Lebensohn, R. A., & Weikusat, I. (2017). Dynamic recrystallization during deformation of polycrystalline ice: Insights from numerical simulations. *Philosophical Transactions of the Royal Society el London A*, **375**(2086), 20150346. **https://doi.org/10.1098/rsta.2015.0346**

Anderson, M., & Kumar, M. (2018). Digital divide persists even as lower-income Americans make gains in tech adoption. Pew Research Center. Retrieved from https://www.pewresearch.org/fact-tank/2018/04/17/digital-divide-persists-even-as-lower-income-Americans-make-gains-in-tech-adoption/.

Cheng, F., & Li, Y. (2020). Cloud computing infrastructure and its effect on police cybersecurity resilience in Asia. *Asian Journal of Information Security*, 12(2), 34-49.

Anderson, T., & Kumar, R. (2021). The impact of IoT integration on cybersecurity resilience in European police departments. *Journal of Cybersecurity Technology and Law*, 9(3), 78-94.

Williams, D., Smith, J., & Lee, P. (2016). Advanced technological infrastructure and cyber threat mitigation in U.S. police departments: A comparative case study. *American Journal of Criminal Justice Technology*, 11(2), 150-168.

Yavuz, S., and Güzel, Ü. (2020). Evaluation of teachers' perception of effective communication skills according to gender. African Educational Research Journal, 8(1): 134-138.

Rahman & Katherine A. Smith, 2022. "**Minding the gap: academic outcomes from pre-college programs**," Education Economics, Taylor & Francis Journals, vol. 30(1), pages 3-28, January.

Kalia, P., & Mishra, G. (2023). Role of Artificial Intelligence in Re-inventing Human Resource Management. In The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part B (pp. 221-234). Emerald Publishing Limited.

Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.

Mizrak, F., & Akkartal, G. R. (2023). Strategic management of digital transformation processes in the aviation industry: Case of Istanbul Airport. In Cases on Enhancing Business Sustainability Through Knowledge Management Systems (pp. 154-177). IGI Global.

Menaka, R. (2022). A Study on Role of Human Resources in Cyber Security In India– With Special Reference to Cyber Risk Management. Journal of Positive School Psychology, 6(2), 4495-4501.

Singh, R., & Sharma, T. (2020). An Explication on Data & Information Security in Human Resource Management System. Vivechan International Journal of Research, 11(1), 54-62.

Gillam, A. R. (2019). Cyber security and human resource development implications for the enterprise. Cyber Security: A Peer-Reviewed Journal, 3(1), 73-92.