Towards Effective Global Information Security Management: Dealing with Cybercrime and Digital Threats for Prosperity

---

Kariuki Muigua

Table of Contents

Towards Effective Global Information Security Management: Dealing with Cybercrime and Digital Threats for Prosperity

Kariuki Muigua*

Abstract

This paper critically discusses the need to strengthen global information security management by dealing with cybercrime and digital threats. The paper argues that cybercrime and other forms of digital threats pose a serious challenge to global information security management and undermine development. It discusses the impacts of cybercrime and digital threats on the global economy. The paper also examines the progress made towards tackling cybercrime and digital threats and challenges thereof. In addition, the paper proposes interventions towards dealing with cybercrime and digital threats towards effective global information security management for prosperity.

1.0 Introduction

Information security has been defined as a risk management discipline that addresses the appropriate protection of confidentiality, integrity and availability of information and the systems used for its storage, processing and transmission[1]. Information security can also refer to the protection of important information against unauthorized access, disclosure, use, alteration or disruption[2]. This concept helps ensure that sensitive data is only available to authorized users, remains confidential and maintains its integrity throughout

* PhD in Law (Nrb), FCIArb (Chartered Arbitrator),OGW, LL. B (Hons) Nrb, LL.M (Environmental Law) Nrb; Dip. In Law (KSL); FCPS (K); Dip. in Arbitration (UK); MKIM; Mediator; Consultant: Lead expert EIA/EA NEMA; BSI ISO/IEC 27001:2005 ISMS Lead Auditor/ Implementer; ESG Consultant; Advocate of the High Court of Kenya; Professor at the University of Nairobi, Faculty of Law; Member of the Permanent Court of Arbitration (PCA) [January, 2025].

[1] United Nations., 'Information Security Policy Directive for the United Nations Secretariat' Available at https://iseek-external.un.org/system/files/iseek/LibraryDocuments/1630-20130314110627399875 4.pdf (Accessed on 07/01/2025)

[2] IBM., 'What is Information Security' Available at https://www.ibm.com/think/topics/information-security (Accessed on 07/01/2025)

its lifecycle[3]. It entails a set of policies, procedures and principles for safeguarding digital data and other kinds of information from unwarranted access[4].

Effective information security management is a vital global endeavour. It has been noted that data and information powers much of the world economy[5]. Data has become a key input in modern economic production alongside other factors of production including land, capital, and labor[6]. For instance, data feeds artificial intelligence algorithms whose predictions power applications ranging from driverless cars, drug testing, and credit provisions among others[7]. Further, it has been noted that data has the power to drive innovative products and services, improve societal well-being and tackle global health and environmental challenges[8]. Data is being harnessed to streamline operations and improve cost efficiency, create tailored products for businesses, and develop new sectors and businesses such as industries that rely on data from satellite information and the emerging area of precision medicine[9]. Due to its advantages, data has been described as the fuel transforming the global economy[10].

In light of the important and increasing role of data in the global economy, cyberattacks targeting personal and organizational information have become more common,

[3] Ibid
[4] Yasar. K., 'Information Security (infosec)' Available at https://www.techtarget.com/searchsecurity/definition/information-security-infosec (Accessed on 07/01/2025)
[5] IBM., 'What is Information Security?' Op Cit
[6] International Monetary Fund., 'The Economics of Data' Available at https://www.imf.org/en/Blogs/Articles/2019/09/23/the-economics-of-data#:~:text=Data%20has%20become%20a%20key,credit%20provision%20to%20ad%20targeting. (Accessed on 07/01/2025)
[7] Ibid
[8] Nurton. J., 'Data: the fuel transforming the global economy' Available at https://www.wipo.int/web/wipo-magazine/articles/data-the-fuel-transforming-the-global-economy-55970#:~:text=Data%20has%20the%20power%20to,protecting%20IP%20and%20other%20rights. (Accessed on 07/01/2025)
[9] Ibid
[10] Ibid

damaging, and costly[11]. Effective global information security management is therefore key in ensuring protection of personal or an organization's important information including digital files and data, paper document, physical media, even human speech - against unauthorized access, disclosure, use or alteration[12]. It ensures confidentiality, integrity, and availability of data and is therefore crucial in safeguarding data and ensuring that it is utilised for its intended purposes[13]. Enhancing global information security management is therefore necessary for posterity.

This paper critically discusses the need to strengthen global information security management by dealing with cybercrime and digital threats. The paper argues that cybercrime and other forms of digital threats pose a serious challenge to global information security management and undermine development. It discusses the impacts of cybercrime and digital threats on the global economy. The paper also examines the progress made towards tackling cybercrime and digital threats and challenges thereof. In addition, the paper proposes interventions towards dealing with cybercrime and digital threats towards effective global information security management for prosperity.

[11] IBM., 'What is Information Security' Op Cit
[12] Ibid
[13] Ibid

2.0 Cybercrime and Digital Threats

Cybercrime has been identified as one of the fastest growing types of crimes globally[14]. The rapid development of digital technologies and the spread of internet access globally not only creates new opportunities for individuals, organizations, and governments but is also fueling cybercrime[15]. This type of crime involves a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target[16]. Further, it has been noted that cybercrime consists of criminal acts committed online by using electronic communications networks and information systems[17]. Cybercrime is a borderless issue that can be classified into several categories including: crimes specific to the internet including attacks against information systems or phishing[18]; online fraud and forgery where large-scale fraud is committed online through instruments such as identity theft, spam and malicious codes[19]; and illegal online content involving acts such as child sexual abuse material, incitement to racial hatred and xenophobia, and incitement to terrorism[20].

[14] Uzoka. NC., 'Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace' Available at https://nigerianjournalsonline.com/index.php/IRLJ/article/viewFile/866/851 (Accessed on 07/01/2025)

[15] Bezborodko. A., 'Cybersecurity threatscape for African countries: Q1 2023–Q3 2024' Available at https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024 (Accessed on 07/01/2025)

[16] Swiatkowska. J., 'Tackling cybercrime to unleash developing countries' digital potential' Available at https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf (Accessed on 07/01/2025)

'[17] European Commission., 'Cybercrime' Available at https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en#:~:text=Cybercrime%20consists%20of%20criminal%20acts,non%2Dlegislative%20actions%20and%20funding. (Accessed on 07/01/2025)

[18] Ibid

[19] Ibid

[20] Ibid

Cybercrime therefore refers to criminal activities that target or use computer systems, computer networks, or network devices[21]. It is mostly committed by cybercriminals or hackers who seek financial gain, although it has been noted that some may also have other motivations such as destroying or damaging electronic systems in wireless networks in order to undermine the operations of organizations and governments[22]. According to the United Nations, cybercrime is an evolving form of transnational crime[23]. This crime is complex in nature since it takes place in the borderless realm of cyberspace and is compounded by the increasing involvement of organized crime groups[24]. It has been noted that perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic, and international response in order to tackle its consequences[25].

Cybercrime and other forms of digital threats are increasing in number, sophistication and cost daily undermining development and the digital potential of most countries[26]. It has been noted that perpetrators of cybercrime are becoming increasingly strategic, resourced and skilled, and are now utilising sophisticated tools of attacks such as ransomware and malware that are very fast in execution and can result in widespread damage[27]. Cybercrime and other forms of digital threats are having devastating impacts on the global economy. For instance, cybercrime can disrupt users from using machines or networks, and prevent businesses from providing services to their customers thus

[21] Lesmana. D., Afifuddin. M., & Adriyanto. A., 'Challenges and Cybersecurity Threats in Digital Economic Transformation' *International Journal of Humanities Education and Social Sciences.*, Volume 2, No. 6 (2023)
[22] Ibid
[23] United Nations Office on Drugs on Crime., 'Cybercrime' Available at https://www.unodc.org/romena/en/cybercrime.html (Accessed on 07/01/2025)
[24] Ibid
[25] Ibid
[26] Uzoka. NC., 'Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace' Op Cit
[27] National Computer and Cybercrime Coordination Committee., 'Cyber Risks, Incidents and Crimes Management' Available at https://nc4.go.ke/research-and-collaboration/ (Accessed on 07/01/2025)

affecting global supply chains[28]. Cybercrime can also be used to spread malware, illegal information, or illegal images undermining the reputation of individuals, businesses, and governments[29]. Other forms of digital threats including cyberbullying and harassment and online fraud pose significant personal and financial risks with cybercriminals leveraging diverse threat vectors such as phishing and identity theft to deceive victims and illicitly obtain money or sensitive information[30].

It has been noted that cybercrime and digital threats have a potential negative impact on economic growth[31]. Cybercrime impacts everyone, from individuals to global corporations, and affects critical infrastructures and governments[32]. Cybercrime causes immense, though not always visible, damage to economies and societies[33]. It is estimated that the cost of cybercrime amounts to nearly $10.5 trillion annually[34]. It is therefore vital to tackle cybercrime and digital threats for prosperity.

3.0 Dealing with Cybercrime and Digital Threats: Promises and Pitfalls

Cybercrime and digital threats continue to present numerous challenges to the global community. These challenges include damage and destruction of data, loss of funds, misappropriation of intellectual property, theft of personal data, lost productivity, and

[28] Lesmana. D., Afifuddin. M., & Adriyanto. A., 'Challenges and Cybersecurity Threats in Digital Economic Transformation' Op Cit
[29] Ibid
[30] Communications Authority of Kenya., 'Cybersecurity Report, January-March 2024' Available at https://ke-cirt.go.ke/wp-content/uploads/2024/04/2023-24-Q3-Cyber-Security-Report.pdf (Accessed on 07/01/2025)
[31] Swiatkowska. J., 'Tackling cybercrime to unleash developing countries' digital potential' Op Cit
[32] World Economic Forum., 'Partnering on cybercrime is taking the fight against cyber threats to new levels' Available at https://www.weforum.org/impact/cybercrime-atlas/#:~:text=Around%2014.4%20billion%20devices%20are,%E2%82%AC10.6%20trillion%20by%202025. (Accessed on 07/01/2025)
[33] Ibid
[34] World Economic Forum., 'Why we need global rules to crack down on cybercrime' Available at https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/ (Accessed on 07/01/2025)

damage to the reputation of individuals, organisations, and governments[35]. In light of these challenges, dealing with cybercrime and digital threats has become vital agenda at the global, regional, and national levels.

At the global level, the *United Nations Convention against Cybercrime*[36] is a landmark global treaty aimed at strengthening international cooperation to combat cybercrime and protecting societies from digital threats. The Convention acknowledges the threat of cybercrime and digital threats to the global community and notes that information and communications technologies, while having enormous potential for the development of societies, create new opportunities for perpetrators and may contribute to the increase in the rate and diversity of criminal activities, and that they may also have an adverse impact on states, enterprises and the well-being of individuals and society as a whole[37]. The Convention notes the importance of protecting the society against cybercrime and digital threats through adopting appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels[38]. In order to effectively tackle cybercrime and digital threats, the Convention seeks to promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively; promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries[39].

[35] Uzoka. NC., 'Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace' Op Cit
[36] United Nations General Assembly., 'United Nations Convention against Cybercrime' A/79/460., Available at https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf (Accessed on 08/01/2025)
[37] Ibid
[38] Ibid
[39] Ibid, article 1

Further, in order to enhance the global response on cybercrime and digital threats, the Convention criminalizes several acts including illegal access of information and communications technology systems, illegal interception of electronic data, interference with electronic data, interference with an information and communications technology systems, misuse of devices, information and communications technology system-related forgery, theft and fraud, non-consensual dissemination of intimate images, laundering of proceeds of crime among others[40]. It requires all states to put in place effective measures including search and seizure of stored electronic data, real-time collection of traffic data, interception of content data, freezing, seizure and confiscation of the proceeds of crime, prosecution of offenders, and protection of witnesses in order to effectively deal with cybercrime and digital threats[41]. Due to the borderless nature of cybercrime and digital threats, the Convention further requires all states to cooperate towards dealing with the global effects of cybercrime and digital threats[42].

The United Nations Convention against Cybercrime is thus a key instrument in tackling cybercrime and digital threats and improving cooperation and coordination among states. It has been pointed out that the Convention could become an important global legal framework for international cooperation on preventing and investigating cybercrime, and prosecuting cybercriminals[43]. It creates an unprecedented platform for collaboration in the exchange of evidence, protection for victims and prevention, while safeguarding human rights online towards effectively and efficiently dealing with

[40] Ibid, chapter II
[41] Ibid, chapter IV
[42] Ibid, chapter V
[43] Wilkinson. I., 'What is the UN cybercrime treaty and why does it matter?' Available at https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter (Accessed on 08/01/2025)

cybercrime and digital threats[44]. It is therefore necessary for all states to implement the Convention in order to combat cybercrime and digital threats and protect human rights in the cyberspace[45].

Dealing with cybercrime and digital threats is also a key agenda in Africa. It has been pointed that as Africa rapidly integrates digital technologies into its socio-political and economic systems, it faces new and complex challenges including cybercrime and digital threats[46]. For instance, there have been cases of tampering with elections in some African countries through cyber interference and misinformation campaigns, and cyberattacks including ransomware attacks targeting critical infrastructure including healthcare and municipal services, underscoring the vulnerabilities associated with increased digital penetration in Africa[47]. Cybercrime also has a significant financial impact on African countries, particularly those with under-protected infrastructures[48]. It is estimated that the financial impact of cybercrime and digital threats in the continent exceeds $4 billion, representing approximately 10 percent of Africa's total Gross Domestic Product (GDP)[49]. It has been noted that most African countries experience cyberattacks including ransomware attacks targeting critical infrastructure such as government infrastructure, hospitals, financial institutions, and internet service providers[50]. Combating cybercrime and digital threats is therefore a key priority for Africa.

---

[44] United Nations., 'UN General Assembly adopts milestone cybercrime treaty' Available at https://news.un.org/en/story/2024/12/1158521 (Accessed on 08/01/2025)
[45] Ibid
[46] ACCORD., 'Emerging cyber conflicts and the role of digital diplomacy in Africa: Trends and strategies' Available at https://www.accord.org.za/conflict-trends/emerging-cyber-conflicts-and-the-role-of-digital-diplomacy-in-africa-trends-and-strategies/ (Accessed on 08/01/2025)
[47] Ibid
[48] African Union., 'African Union strengthens investigation capabilities on virtual assets and cybercrime' Available at https://au.int/en/pressreleases/20240522/african-union-strengthens-investigation-capabilities-virtual-assets-and (Accessed on 08/01/2025)
[49] Ibid
[50] Ibid

The *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*[51] seeks to deal with cybercrime and digital threats in Africa by strengthening cyber security and personal data protection. It sets out key measures towards tackling cybercrime and digital threats in Africa including through ensuring the integrity of electronic transactions, protecting personal data, and strengthening cyber security[52]. Further, in order to combat cybercrime and digital threats, the Convention requires African countries to criminalize acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure; to protect critical infrastructure from cyberattacks; to put in place national cyber security monitoring structures; to prosecute offences; and to foster regional and international cooperation against cybercrime and digital threats[53].

The Malabo Convention is therefore an important legal instrument towards dealing with cybercrime and digital threats in Africa for prosperity. There is need to implement this Convention in order to enhance information security management in Africa.

At a national level, dealing with cybercrime and digital threats is also a vital endeavour for Kenya. The country is facing an increasing risk of cybercrime and digital threats which are compounded by factors such as continued activity by organised cybercrime groups[54]; adoption of more sophisticated tools by ransomware gangs[55]; continued targeted attacks at critical systems and services[56]; adoption of sophisticated phishing and malware kits by

[51] African Union., 'Convention on Cyber Security and Personal Data Protection' Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed on 08/01/2025)
[52] Ibid
[53] Ibid
[54] Communications Authority of Kenya., 'Cybersecurity Report, January-March 2024' Op Cit
[55] Ibid
[56] Ibid

threat actors[57]; and continued targeted attacks at cloud-based supported services and unsecured infrastructure[58]. Kenya has been ranked second in Africa behind Nigeria in terms of financial loss flowing from cybercrime and other digital threats[59]. It has been noted that cybercriminals are continuing to utilise identity theft and phishing to trick victims into disclosing sensitive information resulting in grave financial losses for the country[60].

The Computer Misuse and Cybercrimes Act[61] seeks to combat cybercrime and digital threats in Kenya. In order to achieve this goal, the Act seeks to protect the confidentiality, integrity and availability of computer systems, programs and data; prevent the unlawful use of computer systems; facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes; protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and facilitate international and regional co-operation towards tackling cybercrime[62]. The Act identifies various offences that amount to cybercrime in Kenya including unauthorised access of computer systems, unauthorised interference with computer systems, program or data, unauthorised interception of data, unauthorised disclosure of password or access code, cyber espionage, child pornography, publication of false information online, phishing, cyber harassment, and computer fraud[63]. It requires the state to put in place measures towards detecting, preventing, and prosecuting these crimes[64].

[57] Ibid
[58] Ibid
[59] Ajibade. A., 'Kenya lost $83 million to cybercrime in 2023 and detected 1.1 billion threats from April to June 2024' Available at https://techpoint.africa/2024/10/26/kenya-lost-millions-cybercrime/ (Accessed on 08/01/2025)
[60] Ibid
[61] The Computer Misuse and Cybercrimes Act., Cap 79 C., Government Printer, Nairobi
[62] Ibid, s 3
[63] Ibid, part III
[64] Ibid

The *Data Protection Act*[65] further seeks to enhance information security management in Kenya by regulating the processing of personal data, protecting the privacy of individuals, establishing the legal and institutional mechanism to protect personal data, and providing individuals with rights and remedies to protect their personal data[66].

However, despite laws being put in place at the global, regional, and national levels, cybercrime and digital threats are on the rise globally with devastating impacts on all countries. Cybercrime has emerged as a key global economic and social threat[67]. Cybercriminals are undermining trust in digital platforms, exploiting human empathy and diverting funds from legitimate causes, thereby impacting global stability and prosperity[68]. It is therefore vital to tackle cybercrime and digital threats for prosperity.

4.0 Conclusion

It is imperative to foster effective global information security management. Data has emerged as a critical input in powering modern economic production alongside other factors of production such as land, capital, and labor[69]. Data is vital in powering key sectors of the economy including finance, healthcare, and agriculture among others[70]. Due to the increasing role of information in the global economy and the growth of information and communication systems, cybercrime and digital threats have become more common with cybercriminals exploiting these systems for their personal gain[71]. Cybercrime and digital threats have a devastating impact on individuals, organisations,

[65] Data Protection Act., Cap 411 C., Government Printer, Nairobi
[66] Ibid, s 3
[67] World Economic Forum., 'Why cybercrime spikes in times of global crisis' Available at https://www.weforum.org/stories/2024/02/why-cybercrime-spikes-in-times-of-global-crisis/ (Accessed on 08/01/2025)
[68] Ibid
[69] International Monetary Fund., 'The Economics of Data' Op Cit
[70] Ibid
[71] Bezborodko. A., 'Cybersecurity threatscape for African countries: Q1 2023–Q3 2024' Op Cit

and governments. These effects include damage and destruction of data, loss of funds, misappropriation of intellectual property, theft of personal data, lost productivity, and damage to the reputation of individuals, organisations, and governments[72]. It is therefore necessary to deal with cybercrime and digital threats towards effective information security management.

The global and regional communities have recognised the impact of cybercrime and digital threats and put in place legal regimes towards dealing with these challenges including the *United Nations Convention against Cybercrime*[73]*;* and the *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*[74]. It is imperative to implement these Conventions alongside national laws and policies in order to effectively deal with cybercrime and digital threats. Further, given that cybercrime and digital threats are typically borderless and can impact individuals, organisations, and governments across the world, it is imperative to strengthen global and regional cooperation in order to effectively deal with these challenges[75]. States should therefore enhance collaboration in areas such as technical assistance, capacity-building, exchange of evidence and information, protection of witnesses, and prosecution of crimes in order to effectively combat cybercrime and digital threats[76]. The United Nations identifies international cooperation as crucial towards achieving cyber peace by dealing with the threat of cybercrime[77]. It is also vital for individuals, organisations, and governments to strengthen their cybersecurity capacities in order to mitigate the impacts of cybercrime

[72] Uzoka. NC., 'Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace' Op Cit
[73] United Nations General Assembly., 'United Nations Convention against Cybercrime' Op Cit
[74] African Union., 'Convention on Cyber Security and Personal Data Protection' Op Cit
[75] United Nations., 'UN General Assembly adopts milestone cybercrime treaty' Op Cit
[76] Ibid
[77] United Nations., 'Towards Cyberpeace: Managing Cyberwar Through International Cooperation' Available at https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation (Accessed on 08/01/2025)

and digital threats[78]. This can be realised through enhancing education and training on cybersecurity, designing products including information and communications systems that are secure in order to prevent cybercrime, and putting in place security measures in order to deal with cybercrime and digital threats including hacking and phishing[79].

Dealing with cybercrime and digital threats is an urgent global, regional, and national concern that should be fast-tracked towards global information security management for prosperity.

[78] Swiatkowska. J., 'Tackling cybercrime to unleash developing countries' digital potential' Op Cit
[79] Ibid

References

ACCORD., 'Emerging cyber conflicts and the role of digital diplomacy in Africa: Trends and strategies' Available at https://www.accord.org.za/conflict-trends/emerging-cyber-conflicts-and-the-role-of-digital-diplomacy-in-africa-trends-and-strategies/

African Union., 'African Union strengthens investigation capabilities on virtual assets and cybercrime' Available at https://au.int/en/pressreleases/20240522/african-union-strengthens-investigation-capabilities-virtual-assets-and

African Union., 'Convention on Cyber Security and Personal Data Protection' Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Ajibade. A., 'Kenya lost $83 million to cybercrime in 2023 and detected 1.1 billion threats from April to June 2024' Available at https://techpoint.africa/2024/10/26/kenya-lost-millions-cybercrime/

Bezborodko. A., 'Cybersecurity threatscape for African countries: Q1 2023–Q3 2024' Available at https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024

Communications Authority of Kenya., 'Cybersecurity Report, January-March 2024' Available at https://ke-cirt.go.ke/wp-content/uploads/2024/04/2023-24-Q3-Cyber-Security-Report.pdf

Data Protection Act., Cap 411 C., Government Printer, Nairobi

European Commission., 'Cybercrime' Available at https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en#:~:text=Cybercrime%20consists%20of%20criminal%20acts,non%2Dlegislative%20actions%20and%20funding

IBM., 'What is Information Security' Available at https://www.ibm.com/think/topics/information-security

International Monetary Fund., 'The Economics of Data' Available at https://www.imf.org/en/Blogs/Articles/2019/09/23/the-economics-of-data#:~:text=Data%20has%20become%20a%20key,credit%20provision%20to%20ad%20targeting

Lesmana. D., Afifuddin. M., & Adriyanto. A., 'Challenges and Cybersecurity Threats in Digital Economic Transformation' *International Journal of Humanities Education and Social Sciences*., Volume 2, No. 6 (2023)

National Computer and Cybercrime Coordination Committee., 'Cyber Risks, Incidents and Crimes Management' Available at https://nc4.go.ke/research-and-collaboration/

Nurton. J., 'Data: the fuel transforming the global economy' Available at https://www.wipo.int/web/wipo-magazine/articles/data-the-fuel-transforming-the-global-economy-55970#:~:text=Data%20has%20the%20power%20to,protecting%20IP%20and%20other%20rights

Swiatkowska. J., 'Tackling cybercrime to unleash developing countries' digital potential' Available at https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf

The Computer Misuse and Cybercrimes Act., Cap 79 C., Government Printer, Nairobi

United Nations General Assembly., 'United Nations Convention against Cybercrime' A/79/460., Available at https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf

United Nations Office on Drugs on Crime., 'Cybercrime' Available at https://www.unodc.org/romena/en/cybercrime.html

United Nations., 'Information Security Policy Directive for the United Nations Secretariat' Available at https://iseek-external.un.org/system/files/iseek/LibraryDocuments/1630-20130314110627399875 4.pdf

United Nations., 'Towards Cyberpeace: Managing Cyberwar Through International Cooperation' Available at https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

United Nations., 'UN General Assembly adopts milestone cybercrime treaty' Available at https://news.un.org/en/story/2024/12/1158521

Uzoka. NC., 'Cyber Security and Latest Development: Towards Effective Global Regulation and Governance in Cyberspace' Available at https://nigerianjournalsonline.com/index.php/IRLJ/article/viewFile/866/851

Wilkinson. I., 'What is the UN cybercrime treaty and why does it matter?' Available at https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter

World Economic Forum., 'Partnering on cybercrime is taking the fight against cyber threats to new levels' Available at https://www.weforum.org/impact/cybercrime-

atlas/#:~:text=Around%2014.4%20billion%20devices%20are,%E2%82%AC10.6%20trillion%20by%202025

World Economic Forum., 'Why cybercrime spikes in times of global crisis' Available at https://www.weforum.org/stories/2024/02/why-cybercrime-spikes-in-times-of-global-crisis/

World Economic Forum., 'Why we need global rules to crack down on cybercrime' Available at https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/

Yasar. K., 'Information Security (infosec)' Available at https://www.techtarget.com/searchsecurity/definition/information-security-infosec