Information Ethics and Social Context as Drivers of Cybersecurity Resilience in South Africa's Uneven Digital Landscape

Elekanyani Mukondeleli, Nokuthaba Siphambili and Mmamolele Molema
Council of Scientific and Industrial Research, Pretoria, South Africa

emukondeleli@csir.co.za
nsiphambili@csir.co.za
lmolema@csir.co.za

Abstract: South Africa's rapid digital transformation has expanded socio-economic participation while simultaneously intensifying exposure to cyber risks. These risks are unevenly distributed across society due to persistent digital inequalities, infrastructure gaps and variations in digital literacy. This paper argues that cybersecurity resilience in South Africa cannot be achieved through technical controls alone but must be grounded in information ethics and social context. Using an integrative systemic literature review, the study synthesises research on cybersecurity resilience, information ethics and socio-technical systems within South Africa and comparable environments. The findings reveal recurring socio-ethical patterns in which ethical governance, trust, digital justice, and community-level practices either enable or constrain resilience at the individual, institutional, and societal levels. The paper proposes a Socio-Ethical Cybersecurity Resilience Framework that integrates ethical governance, social behaviour, and institutional responsibility. The framework offers context-sensitive guidance for policymakers, educators and practitioners seeking to strengthen inclusive and sustainable cybersecurity resilience.

Keywords: Cybersecurity resilience, Information ethics, Social context, Digital inequality, South Africa

1. Introduction

South Africa has been experiencing rapid digital change that is affecting how people participate in the economy, education, and governance across the country. Governments have been integrating ICTs into e-governance and e-services to advance a digitalised economy and society as part of global initiatives to expand digitalisation (Alayande et al., 2025). There has been an increase in the use of digital technologies in higher education; this expansion has led to an increase in cybersecurity threats (Henrico & Els, 2025). Policy analysis supports the claim that the nation witnessed a significant increase in cyberattacks affecting individuals, critical infrastructure, and businesses, creating immediate national security and economic threats (Tinonetsana, 2025). However, the risk of cyberattacks is not the same for everyone and is strongly shaped by South Africa's structural inequalities. The results of Digital Transformation Studies reveal that historically disadvantaged communities and institutions are lagging due to a lack of technological expertise, unredressed apartheid policies, poor network coverage, limited access to information technology, and poor infrastructure (Mateko et al., 2025). Within a broader digital access research focus, severe structural inequalities persist in digital use; people have different levels of access and ability to address digital threats (Shibambu & Mojapelo, 2024).

These differences show the limits of relying solely on technical approaches for cybersecurity. Cybersecurity should be viewed as a core matter for a country's socioeconomic development policy and related to the political economy of inequality and risk, not just as a technical IT function (Timcke et al., 2023). Research in African cyber governance also demonstrates that international cybersecurity standards are largely theoretical in the African context despite the presence of "uncertainties of governance mechanisms, political underpinnings and limitations in digital capacity" that have created implementation gaps (Ifeanyi-Ajufo, 2023). To address these issues, this paper adopts an integrative systematic literature review to analyse existing scholarly and policy-oriented studies on cybersecurity, information ethics, and the social context in South Africa and comparable socio-technical environments. Through the systematic identification, analysis, and synthesis of relevant literature, the study identifies recurring socio-ethical patterns that either enable or constrain cybersecurity resilience at individual, community, and institutional levels. Based on these insights, the paper proposes a contextually grounded framework for cybersecurity resilience that integrates ethical governance with social and behavioural considerations. The framework aims to support policymakers, educators and cybersecurity practitioners in designing interventions that are ethically informed, socially inclusive and implementable.

2. Methodology

An integrative systematic literature review examines how information ethics and social context influence cybersecurity resilience in South Africa's uneven digital landscape. An integrative review enables the synthesis

of diverse forms of knowledge by combining empirical studies, theoretical contributions, and policy documents into a coherent analytical framework (Snyder, 2019; Torraco, 2016).

The approach supports the interdisciplinary nature of the research, which spans from cybersecurity, information ethics, governance and socio-technical studies. Because cybersecurity resilience extends beyond technical safeguards to include ethical, behavioural, and structural dimensions, an integrative design enables conceptual integration across disciplinary boundaries. This integrative systematic approach supports theory development and contextual interpretation rather than merely aggregating findings, with a focus on publications from 2019 – 2025. The following databases were used: Scopus, Elsevier, Google Scholar, and Taylor and Francis Online for comprehensive results.

3. Literature Review

3.1 Conceptual and Theoretical Foundations

The integration of cybersecurity resilience, information ethics, and socio-technical perspectives provides a multidimensional understanding of how resilience is shaped by technical capacity, ethical governance, and social context. Cybersecurity resilience is conceptualised as a dynamic, multi-level capability spanning individual, communities and institutions. Information ethics introduces normative principles, such as responsibility, accountability, and fairness, that shape how digital risks and protections are distributed. Socio-technical theory situates cybersecurity practices within broader social, cultural, and structural conditions relevant to South Africa's uneven digital landscape.

Combined, these perspectives frame resilience as a socio-technical and ethically grounded phenomenon by providing the analytical foundation for examining how contextual inequalities influence cybersecurity outcomes.

3.1.1 Cybersecurity resilience

Cybersecurity resilience refers to the capacity of individuals, organisations, communities and states to anticipate, withstand, recover from and adapt to cyber disruptions while maintaining essential functions and protecting the confidentiality, integrity and availability of information systems (NIST, 2022). Unlike traditional risk management approaches that focus primarily on prevention, resilience emphasises adaptive capacity and system continuity in the face of uncertainty (Stella & Monica, 2024).

Recent literature conceptualises resilience as a dynamic and systematic property comprising four interrelated dimensions: preparedness, responsiveness, recovery, and adaptive learning (Leppänen & Simola, 2025). Preparedness includes risk assessment, redundancy planning, and security-by-design measures. Responsiveness entails detection capabilities and incident response coordination. Recovery refers to restoration processes such as data backups and business continuity planning, whereas adaptive learning involves post-incident evaluation and capability improvement to reduce future vulnerabilities. This model emphasises resilience as an ongoing process rather than a fixed state.

3.1.2 Information ethics

Information ethics provides the regulating framework for evaluating how digital systems should be designed, governed and used (Floridi et al., 2020). Within the cybersecurity discourse, three principles are evident: responsibility, accountability, and fairness. Responsibility entails proactive duties to prevent foreseeable harm through secure system design and risk mitigation. Accountability requires transparency and mechanisms for explaining and sanctioning harmful practices. Fairness concerns include equitable treatment and the distribution of digital risk, as well as proactive measures (Khan et al., 2023). These principles are important in situations where power hierarchies exist between technology providers, institutions and users.

Digital justice goes beyond fairness by incorporating distributive and procedural dimensions (Khan et al., 2023). Distributive justice concerns equitable access to secure infrastructure, connectivity and digital education. Procedural justice emphasises inclusive participation in digital policymaking. In unequal contexts such as South Africa, disparities in access, affordability and skills intensify exposure to cyber harms (Shibambu & Mojapelo, 2024). From a resilience perspective, ethical governance strengthens trust, legitimacy, and compliance, which are essential for sustainable cybersecurity practices (Johnson et al., 2024). Without justice-oriented approaches, resilience strategies risk reinforcing existing inequalities by giving privileges to already resourced groups.

3.1.3 Socio-technical and social context perspectives

A socio-technical approach recognises that cybersecurity outcomes emerge from interactions between technology and social practices (Modjadji, 2025). Technical design, economic constraints, institutional trust, cultural norms and everyday usage patterns shape security behaviours. In South Africa, digital inequalities condition both technology adoption and security practices (Mwansa et al., 2025). Things like limited connectivity may prevent timely software updates, while financial constraints will restrict access to secure devices. These structural factors shape realistic security choices.

Cultural norms and institutional trust further mediate resilience. Trust in government and service providers influences compliance with cybersecurity guidance and willingness to share personal data (Ali & Faroque, 2023). If trust is low, individuals may adopt informal, risky workarounds. Risk perception is socially constructed and influenced by lived experience, and communities facing economic challenges may prioritise immediate economic needs over abstract digital risks (Mishra, 2025). Socio-technical perspectives therefore foreground how cultural meaning, social networks, institutional legitimacy and material constraints interact with what they afford technological to produce context-specific patterns of vulnerability and resilience.

3.2 South Africa's Uneven Digital Landscape

3.2.1 Digital inequality and access gaps

Inequalities have clearly defined South Africa's uneven digital landscape. The digital divide is the unequal access to technology, resulting in a lack of literacy, skills, infrastructure, and access for people in rural areas (Modjadji, 2025; Mwansa et al., 2025). Urban areas have been found to have better connectivity than rural areas (Aruleba & Jere, 2022; Mwansa et al., 2025; Shava & Ndebele, 2023). Advances in infrastructure have been centred on urban areas, leaving rural areas at a disadvantage: they lack infrastructure, resulting in limited access and higher costs. Despite advances in technology, information and communication technologies (ICTs) are still not adequately catered for in rural areas, thereby leading to socio-economic issues such as limited access to the internet and basic education (Mwansa et al., 2025).

3.2.2 Digital literacy and cyber risk exposure

South Africa's digital literacy levels are not on par, which poses a high risk of cybersecurity incidents. Digital literacy is closely linked to how a country or community responds to cyber risks (Amoresano & Yankson, 2023). Humans are the number one cause of data breaches (Amoresano & Yankson, 2023). Therefore, due to a lack of infrastructure, this further affects an individual's literacy and ability to be cyber-aware. Human behaviour is the weakest link because people act as a human firewall, preventing cybersecurity threats. Due to South Africa being a high target for cyberattacks such as ransomware, organisations are bound to face data breaches because of a lack of literacy programs. Due to the proliferation of advanced technology, artificial intelligence (AI) has created new vulnerabilities, including the threat posed by deepfake technology (Folorunsho & Boamah, 2025; Mahlasela et al., 2024; Ratnawita, 2025). Anyone with the knowledge and skill can thus generate AI images, videos, and sound, which are then used to deceive people (Mahlasela et al., 2024).

Cybersecurity awareness is a need due to advances in technology. Organisations create and implement cybersecurity awareness initiatives to educate employees and equip them to act should they face a cyber incident (Abrahams et al., 2024). This results in low coverage, where not everyone sees cybersecurity as their responsibility but rather as an ICT's responsibility (Panteli et al., 2025).

3.2.3 Structural and historical inequalities

Historically, in South Africa, digital inequalities have persisted due to the country's social and political history (Modjadji, 2025). There have been infrastructure disparities due to policies implemented during the apartheid era (Modjadji, 2025). Due to unequal access to education, ICTs and the apartheid era, access to the digital infrastructure technologies has left other communities marginalised. Structural and historical inequalities have been deeply rooted in apartheid. The digital divide has amplified this; it not only affects literacy levels and access to technology but also shapes how communities can improve their skills and lives (Mugunzva & Manchidi, 2025). This affects communities' ability to improve their lives, as they are unable to leverage ICTs to advance their social and economic well-being. Digital practices are still deeply shaped by historical inequalities and structural constraints (Mugunzva & Manchidi, 2025).

Due to rural-urban disparities, many rural areas have limited access to infrastructure, including unreliable electricity and network connectivity, thereby affecting internet access (Anil & Disparities, 2024; Khan et al.,

2023). This has led to situations in which some communities use legacy systems. These legacy systems create vulnerabilities, and without the right skills, South Africa is left vulnerable to cyberattacks. These legacy systems result in outdated software, leading to a lack of updates or new patches. Disparities in access to technology and internet connectivity, often rooted in socioeconomic status, mean that rural areas and underserved communities are less equipped to handle cyber threats (Khan et al., 2023; Nthambeleni & Motadi, 2025). There is a need for digital inclusion across all communities to ensure inclusivity and enable communities to address cyber threats (Layne et al., 2026).

3.3 Information Ethics as a Driver of Cybersecurity Resilience

3.3.1 Ethical responsibility and accountability

Information ethics helps make cybersecurity stronger by showing that keeping things secure is shared now with many layers, including "techno-centric, human-centric, organisational (intra and inter) and social centric perspectives", an onion-shaped framework in which senior leadership plays an important role in fostering responsible cybersecurity (Panteli et al., 2025). From a public-interest perspective, ethical rules treat cybersecurity as a benefit to everyone, requiring analysis of core ethical principles and values of liberal democracy, such as privacy, communication, freedom, and fairness, alongside ethical guidelines that change how institutions operate (Miller & Bossomaier, 2024). For people working in cybersecurity, professional ethics makes it clear that they are responsible to the public, clarifying their duties and what good ethical behaviour looks like, which directly links ethical conduct to resilient outcomes (Vallor et al., 2016). At the institutional level, resilience depends on strong governance and policy frameworks that ensure compliance and protect sensitive data. Studies in higher education argue that cohesive governance is essential to mitigate risks, ensure compliance, and protect academic research, financial, and personal data, especially amid threats such as ransomware and data breaches (Ali, 2025). Governmental obligations arise because cybersecurity has become a strategic priority, with attacks blurring the traditional distinction between crime and acts of war. This means governments need to create rules and make ethical changes to protect critical systems and democratic processes (Miller & Bossomaier, 2024).

3.3.2 Fairness, inclusion, and digital justice

Fairness, inclusion, and digital justice are important parts of cybersecurity because effective protection must honour fundamental values such as equality, fairness, freedom, and privacy (Kirichenko et al., 2020). Unequal cyber protection worsens existing social inequalities. Digital exclusion keeps economic, educational and social gaps in place, making cybersecurity and digital access key parts of social justice (DavethanTech, 2025). At the technical level, algorithmic tools used in cybersecurity can reflect or amplify biases, leading to unfair targeting or exclusion, underscoring the ethical problem of unequal protection based on discrimination (Whittaker, 2020). These differences show the importance of inclusive security frameworks, as cybersecurity is understood as a matter of equity, fairness, and inclusivity, requiring systems that protect individuals, particularly the most vulnerable, such as people with disabilities, older people, children, and gender minorities (Duhem, 2024). These findings show that fairness and digital justice are not just nice ideas but important ethical principles to ensure that cybersecurity works for every user equally.

3.3.3 Ethical governance in cybersecurity

Cybersecurity ethical governance calls for frameworks that mitigate risks, ensure compliance, and protect data, underscoring the importance of robust cybersecurity policies for resilient institutions (Ali, 2025). Research supports the adoption of clear cybersecurity policy frameworks backed by "privacy-by-design principles", adaptive regulations, and coordinated action to address global cybercrime and data privacy challenges beyond generic controls (Kirichenko et al., 2020).

Ethics in cybersecurity means respecting basic values such as equality, fairness, freedom, and privacy, and using real-life examples to guide decisions (Kirichenko et al., 2020). From this governance perspective, POPIA extends beyond being compliance-focused to hands-on, proactive data stewardship: a review of how this works in South Africa points to real steps like staff training, risk checks, and meeting international data protection standards, showing a transition from theoretical discourses to empirical and sector-specific research on POPIA (Sema et al., 2025). Simultaneously, studies for professionals incorporate ethics, law, and policy dimensions by showing how responsibility rules connect to daily controls and by mapping how governance structures embed duties and align with regulatory obligations (Priyadarshini & Cotton, 2022).

3.4 Social Context and Cybersecurity Behaviour

3.4.1 Trust, risk perception, and secure practices

Humans are often seen as the number one cause of data breaches (Amoresano & Yankson, 2023). Therefore, trust, risk perception and secure practices are crucial to create a cyber-resilient economy. Trust is crucial in cybersecurity, where the zero-trust model is in place. The zero trust model states that "trust no one, verify all." Users tend to trust that technology will inherently protect them from any attacks, thereby lacking the right measures to implement in their personal lives (Nasir et al., 2024). While trust is important, it is worth noting that in cybersecurity, trust can lead to reduced efforts to protect oneself (De Kimpe et al., 2022). An individual's perception of risk evaluates how they are likely to respond to risks (Andersson et al., 2023). Therefore, this impacts how one protects themselves, the community, and the organisations they work for. When one feels at risk, they are more likely to take proactive measures to protect themselves.

The community one lives in plays a significant role in how they adopt and take secure practices to protect themselves. The organisational culture also plays a significant role in terms of how one implements secure practices at the workplace and in their personal lives (Panteli et al., 2025). The environment one lives in also determines the type of practices one employs. For example, if one stays in a literate community that values implementing secure practices, they are more likely to be cyber-resilient. Due to the digital divide, disadvantaged communities are less likely to adopt best practices for securing their cyberspace.

3.4.2 Cultural norms and everyday digital practices

Cultural norms play a significant role in terms of how an individual protects themselves. Inequitable disparities play a significant role in how best practices are implemented (Modjadji, 2025). People in rural areas are less likely to adopt best practices due to the digital divide. This thus affects how cyber-resilient one is and how they adopt best practices in their lives (Djatmiko et al., 2025). A community that values or is deeply rooted in being resilient is more likely to adopt secure best practices. An organisation with a cybersecurity culture is more likely to ensure that its employees adopt secure best practices (Panteli et al., 2025). There is a need for a nationwide initiative to teach communities how to adopt best practices to ensure their online safety.

3.4.3 Community-level cybersecurity resilience

For a community to be resilient, it means that a community or group of people builds and ensures they are equipped with the right skills and knowledge to prevent cyber threats (Jarjoui et al., 2024). This includes training and awareness initiatives to build a cyber-resilient community. This also includes initiatives set up by the government and organisations to build community-level cybersecurity resilience (Jarjoui et al., 2024). This includes creating and adopting policies to protect communities. This also includes training and awareness initiatives undertaken by organisations to educate employees on how to respond to incidents within the organisation and in their personal lives.

When an employee adopts the right practices in their personal lives, they are more likely to implement the same initiative at their workplace (Aksoy, 2024; Kuiper, 2025). A collective effort is required for a community to be cyber resilient. Humans are the number one cause of breaches; therefore, it is essential to ensure a strong human firewall is in place. Furthermore, this leads to a community with a shared responsibility for protecting its community or organisation.

4. Proposed Socio-ethical Cybersecurity Resilience Framework

This study proposes a Socio-Ethical Cybersecurity Resilience Framework that positions resilience as a multi-level, socio-technical construct shaped by ethical governance, social behaviour, and institutional responsibility. Contemporary resilience scholarship emphasises that cybersecurity resilience extends beyond technical robustness to include adaptive capacity, governance maturity and human behaviour (Leppänen & Simola, 2025; Linkov et al., 2022). At the same time, the digital ethics literature underscores the importance of embedding responsibility, accountability, and justice within the digital governance system to prevent unequal harm (Floridi et al., 2020; Stahl, 2021).

The South African context is characterised by persistent digital inequality, uneven infrastructure, and socio-economic differences, with cyber risk exposure distributed unevenly across these groups. A resilience model that ignores ethical governance and social context risks reinforcing existing vulnerabilities. The proposed framework therefore integrates three interdependent pillars: ethical governance, social behaviour and

institutional responsibility, which will collectively shape cybersecurity resilience at individual, community and institutional levels.

4.1 Framework Components

Framework Components	What they are
4.1.1 Ethical Governance	Ethical governance refers to the normative and regulatory foundations that guide cybersecurity decision-making. It incorporates principles of responsibility, accountability, fairness, and digital justice that ensure cybersecurity policies do not merely comply with legal requirements but also address distributive and procedural inequalities (Floridi *et al.*, 2020). Responsibility covers proactive harm and risk mitigation. Accountability requires transparent mechanisms for oversight and redress. Fairness and digital justice demand that protective measures and resources be distributed equally, particularly in addressing structural inequalities. Ethical governance, therefore, serves as the normative anchor of resilience, shaping institutional conduct and influencing public trust.
4.1.2 Social Behaviour	Every day, digital practices, trust relationships, cultural norms and risk perception significantly shape cybersecurity resilience. Socio-technical research illustrates that security outcomes emerge from interactions between technological systems and human behaviour rather than technical design alone (Baxter & Sommerville, 2011; Leppänen & Simola, 2025). In South Africa, gaps in digital literacy, affordability of connectivity and access to technological devices influence the adoption of safe practices. Thus, trust in institutions further mediates compliance with cybersecurity guidance. Social behaviour, therefore, represents the human dimension of resilience, highlighting that awareness, education and culturally responsive engagement strategies are essential components of sustainable cybersecurity capacity
4.1.3 Social Behaviour	Institutional responsibility encompasses the obligations of state entities, private organisations, and public institutions to create enabling conditions for resilience. This includes developing coherent cybersecurity policies, investing in secure infrastructure, building capacity, and implementing transparent incident response mechanisms. Resilient institutions demonstrate adaptive governance and intersectoral, continuous learning from cyber incidents (Linkov, Trump, and Keisler, 2022). In an uneven digital environment, institutional responsibility also entails prioritising marginalised communities in capacity development initiatives. By embedding ethical governance into operational structures, institutions serve as a critical enabler of systemic resilience.

4.1.1 Conceptual structure of the framework

Figure 1: Socio-Ethical Cybersecurity Resilience Framework

Application in the South African Context: In South Africa's uneven digital landscape, persistent digital inequality, infrastructure disparities, and trust deficits shape vulnerability exposure and resilience capacity (Shibambu & Mojapelo, 2024). The framework, therefore, calls for integrating cybersecurity strategies with digital inclusion efforts, strengthening ethical oversight, and promoting context-sensitive awareness initiatives.

Implications for Policymakers, Educators and Practitioners:

- Policymakers: Align cybersecurity governance with digital justice and broader socio-economic development goals.
- Educators: Combine cybersecurity literacy with ethical and civic education.
- Practitioners: Design user-centred security, transparent communication practices and ethical risk assessments that account for socio-economic context.

5. Discussion

The findings of this study have important theoretical implications for cybersecurity resilience. By integrating information ethics and socio-technical perspectives, the paper advances resilience theory beyond predominantly technical and systems-engineering approaches towards a normatively grounded, socially embedded framework. Contemporary resilience literature emphasises adaptive capacity, recovery and continuity (Leppänen & Simola, 2025; Linkov et al., 2022) yet often under-theorises how ethical governance and distributive justice shape resilience outcomes. Drawing on recent work in digital ethics and governance (Linkov et al., 2022; Stahl, 2021), this study reframes cybersecurity resilience as a socio-ethical construct in which responsibility, accountability, fairness and trust are constitutive rather than peripheral elements.

The study highlights that strengthening cybersecurity resilience in South Africa requires context-sensitive and justice-oriented interventions. Empirical research shows that digital inequality, infrastructure deficits and uneven literacy significantly mediate vulnerability exposure in the Global South context (Shibambu & Mojapelo, 2024). Consequently, compliance-driven cybersecurity programmes are insufficient without parallel investments in inclusive digital capacity building and ethical governance mechanisms. Embedding principles such as privacy-by-design, transparent oversight and community-level awareness into institutional practice enhances public trust and supports sustainable behavioural change (Kelly, 2024). The proposed socio-ethical framework, therefore, offers policymakers, educators, and practitioners an integrated approach that aligns cybersecurity strategy with broader socio-economic development and digital inclusion objectives.

In terms of the contribution of Global South cybersecurity literature, this study addresses a persistent gap in scholarship that often privileges Global North regulatory models and technical standards while under examining structural inequality and normative governance in developing contexts (Ifeanyi-Ajufo, 2023; Timcke et al., 2023). By foregrounding ethical governance and social context as drivers of resilience, the paper provides a contextually grounded and transferable analytical model applicable to other digitally unequal societies. The socio-ethical resilience framework thus contributes to emerging debates on decolonising cyber governance scholarship and promoting justice-centred digital security paradigms in Africa and comparable socio-technical environments.

6. Conclusion

This paper argues that cybersecurity resilience in South Africa cannot be fully grasped or enhanced solely through technical measures. Located within a highly uneven digital environment shaped by historical inequalities, infrastructural gaps, and disparate levels of digital literacy, cyber risk is distributed across society in socially patterned and ethically mediated ways.

The proposed Socio-Ethical Cybersecurity Resilience Framework advances both academic understanding and real-world application by treating ethical governance, social behaviour, and institutional accountability as mutually reinforcing foundations of resilience. In this way, the paper enriches Global South cybersecurity debates by placing structural inequality and justice at the centre of analysis rather than treating them as secondary contexts. In South Africa and comparable contexts, enhancing cybersecurity resilience thus depends on aligning governance arrangements, digital inclusion efforts, and behavioural initiatives within a unified ethical framework. In the end, resilience in an unequal digital landscape is not simply a matter of technical capability, but of fair protection, confidence in institutions, and a digitally driven transformation that is deeply rooted in society.

Ethics declaration: The study employed previously published peer-reviewed journal articles and, as no human subjects were involved, ethical approval was not required.

AI Usage Declaration: Generative artificial intelligence (AI), specifically large language models (LLMs), was used to enhance writing, correct grammatical errors, and provide summaries of literature to disseminate information. No tools were used to write original content. AI tools used to aid the writing process include Grammarly, Writefull, and ChatGPT.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100–119.

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, *7*(1), 96–110.

Alayande, A., Segun, S., Junck, L., Adeleke, F., Abdella, S., Adams, R., Gaffley, M., & Salami Editor, F. (2025). *Emerging technology policies and democracy in Africa and Zambia in focus Contributors*.

Ali, G. M. (2025). *Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance Research Review Article*.

Ali, K. S., & Faroque, A. R. (2023). *Addressing the complexity of the digital divide and the role of government in addressing it: Role of government in bridging the digital divide*.

Amoresano, K., & Yankson, B. (2023). Human error-a critical contributing factor to the rise in data breaches: a case study of higher education. *Holistica Journal of Business and Public Administration*, *14*(1), 110–132.

Andersson, I., Bjursell, L., & Palm, I. (2023). *Hack the Human: A qualitative research study exploring the human factor and social engineering awareness in cybersecurity and risk management among Swedish organizations.*

Anil, K., & Disparities, G. (2024). Bridging the Gap: Understanding and Addressing Rural-Urban Disparity. *Vigyan Varta*, *5*(9), 144–146.

Aruleba, K., & Jere, N. (2022). Exploring digital transforming challenges in rural areas of South Africa through a systematic review of empirical studies. *Scientific African*, *16*, e01190.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

DavethanTech. (2025). *The Role of Digital Inclusion & Cybersecurity in Social Justice*.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796–1808.

Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance. *Sustainability (Switzerland)*, *17*(7). https://doi.org/10.3390/su17072908

Duhem, M. (2024, October 30). *Building an Inclusive Cybersecurity Framework: A Must for Today's Digital World*.

Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to Design AI for Social Good: Seven Essential Factors. *Science and Engineering Ethics*, *26*(3), 1771–1796. https://doi.org/10.1007/s11948-020-00213-5

Folorunsho, F., & Boamah, B. F. (2025). Deepfake technology and its impact: ethical considerations, societal disruptions, and security threats in ai-generated media. *International Journal of Information Technology and Management Information Systems*, *16*(1), 1060–1080.

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice*, *6*(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960

Jarjoui, S., Murimi, R. M., & Murimi, R. K. (2024). Communities Agency and Resilience: A perspective Addressing Tragedy of the Cyber Commons. *Cyber Defense Review*.

Johnson, Rob., Weiss, Martin., & Solomon, Michael. (2024). *Auditing IT infrastructures for compliance*. Jones & Bartlett Learning.

Kelly, B. (2024). *To Build Digital Trust, Start with Resiliency*. https://www.networkworld.com/article/

Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*, 1.

Kirichenko, A., Christen, M., Grunow, F., & Herrmann, D. (2020). Best Practices and Recommendations for Cybersecurity Service Providers. In *International Library of Ethics, Law and Technology* (Vol. 21, pp. 299–316). Springer Science and Business Media B.V. https://doi.org/10.1007/978-3-030-29053-5_15

Kuiper, M. E. (2025). There Is No Quick Fix: Compliance Officers' Views on Organizational Behavioral Change. *Journal of Business Ethics*, 1–26.

Layne, A., Liu, L., Akanaga, C., & Comert, G. (2026). Why Race and Place Matter: Examining the Intersection of Cybersecurity and Digital Equity. *Journal of Black Studies*, *57*(1), 28–50.

Leppänen, T., & Simola, J. (2025). *Identification of the Emerging Sources of Cybersecurity Threats*.

Linkov, I., Trump, B. D., & Keisler, J. (2022). Risk and resilience must be independently managed. *Nature*, *555*. https://link.gale.com/apps/doc/A529350364/AONE?u=anon~74700a3b&amp

Mahlasela, O., Baloyi, E., Siphambilie, N., & Khan, Z. C. (2024). *Artificial Intelligence Impact on the Realism and Prevalence of Deepfakes*.

Mateko, F. M., Dowelani, M., & Sinamano, R. (2025). Digital Inequality and Transformation in South African Higher Education During COVID-19: A Comparative Analysis of Historically Disadvantaged and Historically Advantaged Universities. *Higher Education Policy*. https://doi.org/10.1057/s41307-025-00416-0

Miller, S., & Bossomaier, T. (2024). *Cybersecurity, Ethics, and Collective Responsibility*.

Mishra, N. (2025). *Cybersecurity and International Trade*.

Modjadji, M. M. (2025). *Bridging divides: tackling technological change, inequality, and digital illiteracy in a fragmented South Africa*.

Mugunzva, F. I., & Manchidi, N. H. (2025). Mapping Digital Literacy Thresholds in South African Higher Education and the Implications for Entrepreneurship Education in an Industry 4.0 Paradigm. *Administrative Sciences*, *15*(10), 396.

Mwansa, G., Ngandu, M. R., & Mkwambi, Z. (2025). Bridging the digital divide: exploring the challenges and solutions for digital exclusion in rural South Africa. *Discover Global Society*, *3*(1), 54.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. *Spectrum of Engineering Sciences*, 420–454.

NIST. (2022). *2021 cybersecurity and privacy annual report*. https://doi.org/10.6028/NIST.SP.800-220

Nthambeleni, N. B., & Motadi, M. S. (2025). Digital globalisation and educational inequalities access, infrastructure, and pedagogy in marginalised regions. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *7*(5), 496–509.

Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being responsible in cybersecurity: A multi-layered perspective. *Information Systems Frontiers*, 1–19.

Priyadarshini, I., & Cotton, C. (2022). *Cybersecurity Ethics, Legal, Risks and Policies*.

Ratnawita, R. (2025). Cybersecurity in the AI era measures deepfake threats and artificial intelligence-based attacks. *Journal of the American Institute*, *2*(2), 180–189.

Sema, G. G., Owolawi, P. A., & Olugbara, O. O. (2025). Protection of Personal Information Act in Practice: A Systematic Synthesis of Research Trends, Sectoral Applications, and Implementation Barriers in South Africa. In *Sustainability (Switzerland)* (Vol. 17, Number 19). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/su17198529

Shava, E., & Ndebele, N. C. (2023). Data marginalization in South Africa: A quest for inclusive digital participation. *Social Sciences and Education Research Review*, *10*(2), 122–131.

Shibambu, A., & Mojapelo, S. M. (2024). The status of digital and information literacies in South Africa from 2016 to 2022: a literature review. *Global Knowledge, Memory and Communication*, *74*(7–8), 2572–2584. https://doi.org/10.1108/GKMC-04-2023-0142

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stahl, B. C. (2021). *Artificial Intelligence for a Better Future*. http://www.springer.com/series/13811

Stella, R. M., & Monica, I. (2024). *Institutionalizing Cybersecurity Policies Through Digital Communication Strategies. Assessing the Digital Nodality of Cybersecurity Agencies in Italy and France*. 113–144. https://doi.org/10.1483/113154

Timcke, S., Gaffley, M., & Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication (AJIC)*, (32), 1–28. https://doi.org/10.23962/ajic.i32.16949

Tinonetsana, F. (2025). *Addressing the Rise of Cyberattacks in South Africa*. www.hsrc.ac.za

Torraco, R. J. (2016). Writing Integrative Reviews of the Literature. *International Journal of Adult Vocational Education and Technology*, *7*(3), 62–70. https://doi.org/10.4018/ijavet.2016070106

Vallor, S., William, J., & Rewak, S. J. (2016). *An Introduction to Cybersecurity Ethics*. https://techethics.ieee.org